(51) Int. Cl. 2: G 06 F 15-30
G 07 G 5-00
G 07 F 7-08

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

DT 25 27 784 A1

(11) Offenlegungsschrift 25 27 784

(21) Aktenzeichen: P 25 27 784.3
(22) Anmeldetag: 21. 6. 75
(43) Offenlegungstag: 15. 1. 76

(30) Unionspriorität:
(32) (33) (31) 25. 6. 74 USA 483084

(54) Bezeichnung: Kommunikationssystem mit mißbrauchgeschützter Kontendatei

(71) Anmelder: International Business Machines Corp., Armonk, N.Y. (V.St.A.)

(74) Vertreter: Lewit, L., Dipl.-Ing., Pat.-Ass., 7030 Böblingen

(72) Erfinder: Anderson, Thomas George, Los Altos; Boothroyd, William Arnold; Frey, Richard Carl; San Jose; Calif. (V.St.A.)

DT 25 27 784 A1

© 12. 75 509 883/872 36/80

2527784

Böblingen, den 16. Juni 1975
lw-fr

Anmelderin: International Business Machines Corporation, Armonk, N.Y. 10504

Amtliches Aktenzeichen: Neuanmeldung

Aktenzeichen der Anmelderin: SA 973 016

Kommunikationssystem mit mißbrauchgeschützter Kontendatei

Die Erfindung betrifft ein Kommunikationssystem mit mißbrauchgeschützter, zentraler Kontendatei. Solche für die Wirtschaft entwickelte Systeme dienen zur Ausführung von von einem Benutzer angeforderten Geldtransaktionen und sollen leicht bedienbar sein. Ein Beispiel dafür ist eine Scheckkassenmaschine. Eine solche Maschine liest Daten von einem in die Maschine eingelegten Scheck und gibt Bargeld in der Höhe der Eintragung auf dem Scheck aus, wenn der Scheck in Ordnung befunden wird. Andere Systeme wurden für die Benutzung in Verbindung mit Kreditkarten entwickelt.

Ein Kreditkartensystem speichert Information über Kreditkartenkonten in einer zentralen Datenbasis. Wenn eine Kontonummer von einer entfernten Datenstation (Terminal) eingegeben wird, liefert das System Information über das Konto. Das System kann z. B. angeben, daß die Karte abgelaufen ist, daß sie gestohlen wurde oder kann den verfügbaren Kreditbetrag in Dollars angeben. Nachdem eine Transaktion abgeschlossen ist, bringt das System die gespeicherte Information auf den neuesten Stand, so daß die Transaktion berücksichtigt wird.

Andere häufig von Banken zur Erweiterung ihres Kundendienstes während der Zeiten starker Geschäftstätigkeit oder den Schließungszeiten der Bank benutzte Kreditkartensysteme gestatten die Ausgabe von Bargeld oder die Annahme von Einlagen über eine Systemstation. Zu einem typischen derartigen System gehört eine

Einrichtung zum Empfang und Lesen von Information von einer Kreditkarte, eine Tastatur, ein Bildanzeigegerät und Öffungen zur Eingabe und Ausgabe von Belegen. Die Station arbeitet in Verbindung mit einer Datenbasis oder als unabhängige Einheit. Erhöhte Sicherheit für die Ausgabe von Bargeld ohne menschlichen Eingriff erhält man durch Ausgabe von persönlichen Codezahlen mit einer Kreditkarte. Eine Kreditkartentransaktion wird dann nur möglich, wenn eine der von der Kreditkarte gelesenen Kontonummer entsprechende Codezahl über die Tastatur eingegeben wird. Diese verlangte Entsprechung verhindert, daß ein Dieb oder auch nur der Finder einer Kreditkarte Bargeld von einer Station empfängt. Wenn eine Station mit einer Datenbasis zusammenarbeitet, kann die Entsprechung zwischen Kontonummern und Codenummern beliebig gewählt werden, häufig läßt sich die Codenummer jedoch von der Kontonummer entsprechend einem vorgegebenen Code ableiten. Diese vorgegebene Beziehung ermöglicht der unabhängigen Station die Prüfung der Codezahl durch algorithmische Zuordnung der Codezahl zur Kontonummer.

Während diese doppelte Identifizierungstechnik durch Kreditkarten- und Codenummer die Sicherheit der Bargeldausgabestationen verbessert, gibt es immer noch schwache Punkte, die ausgenutzt werden können, um Zugang zu den großen Geldmengen zu erhalten, die in den Stationen gelagert sind. Es kann z. B. nötig sein, eine beträchtliche Anzahl von Computeroperatorn, Programmmierern, Analytikern und anderen Personal an der Datenbasis zu beschäftigen, die mindestens begrenzten Zugang zu den in der Datenbasis gespeicherten Informationen haben. Für alle diese Leute besteht die Möglichkeit, Listen mit Kontonummern und entsprechenden Identifizierungsnummern zusammenzustellen, die dann in Verbindung mit gefälschten oder gestohlenen Kreditkarten dazu benutzt werden, Bargeld zu bekommen.

Ein ebenso ernstes Problem ist die Sicherheit des Verschlüsselungsalgorithmus für Stationen, die unabhängig arbeiten können. Für

die tägliche Unterstützung der Bargeldausgabestationen ist eine beträchtliche Anzahl von Bedienungs- und Wartungspersonal erforderlich. So können z. B. ein oder zwei Leute an jeder Zweiggstelle internen Zugang zu den Geldausgabestationen haben. Oft kennen diese Leute auch den Verschlüsselungscode für die normale Wartung. Andererseits kann mit nur wenig Schulung dieses Personal lernen, sich den Schlüssel durch Messen elektrischer Signale an der inneren Schaltung zu beschaffen. Wenn der Schlüssel einmal bekannt ist, kann man eine Korrespondenz zwischen einer großen Anzahl von Kontonummern und Identifizierungsnummern herstellen.

Ein anderes mögliches Sicherheitsproblem entsteht bei der Übertragung von Kontoinformation und Idenfizierungsinformation zwischen einer Station und einer Datenbasis. Diese Übertragungen laufen oft über öffentliche Nachrichtenleitungen und können daher durch eine große Anzahl von Leuten überwacht werden. Die Verschlüsselung wird oft zur Verbesserung der Sicherheit angewandt, wer aber den Code entschlüsseln oder Zugang zum Code erhalten kann, kann eine Korrespondenzliste zwischen Kreditkartenkontoinformation und Identifizierungszahlen herausziehen und zusammenstellen durch Überwachung dieser Übertragungen. Durch Aufbau eines simulierten Verkehrs mit einer Station kann eine Person außerdem Zugang zur Datenbasis bekommen und betrügerischerweise Beträge innerhalb der Konten der Datenbasis übertragen. Während also konventionell diese doppelte Identifizierungstechnik benutzende Systeme gegen gemeinen Diebstahl gut geschützt sind, sind sie nicht gleichermaßen gegen den versierten Dieb geschützt, der Kenntnisse in der modernen Datenverarbeitung hat.

Der Erfindung liegt daher die Aufgabe zugrunde, bei Geldtransaktionen mit Hilfe des eingangs beschriebenen Kommunikationssystems die Sicherheit gegen Mißbrauch durch Verbesserung der Verschlüsselung zu erhöhen.

Diese Aufgabe wird erfindungsgemäß durch die im Kennzeichen des Hauptanspruchs beschriebene Einrichtung gelöst.

Die Erfindung hat den Vorteil, daß ein Mißbrauch des Terminals durch einen Finder oder Dieb eines Schecks, oder einer Kreditkarte mit hoher Sicherheit vermieden wird. Dies gilt selbst dann, wenn es dem Betrüger gelingt, Kenntnis von der Zuordnung zwischen persönlicher Identifizierungsnummer (Codezahl) und Kontonummer zu erhalten.

Weitere technische Vorteile sowie vorteilhafte Weiterbildungen der Erfindung sind den nachstehenden Ausführungen zu entnehmen.

Das erfindungsgemäße Transaktionsausführungssystem enthält ein Datenverarbeitungssystem mit einer Datenbasis aus gespeicherten Informationen für viele Konten und mehrere Transaktionsstationen. Das Datenverarbeitungssystem genehmigt oder verbietet angegebene Transaktionen, verändert gespeicherte Konteninformation auf den richtigen Kontostand für ausgeführte Transaktionen und liefert Unterstützungsinformation für die Stationen. Die Transaktionsstationen sind unabhängige Einheiten, die zur Kommunikation von verschiedenen Stellen mit dem Datenverarbeitungssystem verbunden werden. Jede Datenstation enthält verschiedene Untersysteme, und zwar ein Belegverarbeitungssystem für die Bestätigung von Auszahlungen oder Transaktionen, ein Kreditkartenlesesystem, ein EDV-Kommunikationssystem, ein Benutzer-Kommunikationssystem und ein Betriebssteuersystem einschließlich eines programmierbaren Mikroprozessors.

Das Belegverarbeitungssystem enthält eine Geldspeichereinrichtung, eine Transporteinrichtung zur Ausgabe von Bargeld an einen Benutzer unter der Überwachung und Kontrolle des Mikroprozessors und einen Transaktions-Beleggeber, der unter Steuerung des Mikroprozessors gedruckte Bestätigungen ausgibt. Das Kreditkartenlesesystem läuft unter der Steuerung des Mikroprozessors und empfängt und liest Kreditkarten der Benutzer, die entweder zu-

rückgegeben oder nach der Verarbeitung der Transaktionsanforderung einbehalten werden. Das EDV-Kommunikationssystem bildet eine Schnittstelle für die richtige Übertragung von Information zwischen einer Station und einer EDV-Anlage nach vorgegebenem Kommunikationsformaten. Das Benutzer-Kommunikationssystem reagiert auf Befehle des Mikroprozessors und kontrolliert den Zugriff des Benutzers zur Station und enthält eine Tastatur zum Empfang der Befehle des Benutzers sowie ein Datensichtgerät zur wechselseitigen Anleitung des Benutzers.

Wenn ein Benutzer eine Transaktion ausführen will, muß er eine Kreditkarte in eine Station einlegen und dann seine persönliche Identifizierung und die Transaktionsanforderungsinformation über die Tastatur eingeben. Die Station codiert dann optionell einen ausgewählten Teil der Kreditkarteninformation mit Hilfe eines ersten Codierschlüssels, um eine codierte Identifizierungsinformation zu erhalten, die auf Korrospondenz mit einem ausgewählten Teil der über die Tastatur eingegebenen Identifizierungsinformation überprüft wird. Wenn eine vorher bestimmte Korrespondenz nicht vorliegt, wird die Transaktion beendet und eine entsprechende Mitteilung an die Datenverarbeitungsanlage gesendet. Die Antwort der Anlage besagt, was mit der Karte zu geschehen hat, die dann wahlweise zurückgegeben und einbehalten wird. Wenn die Korrespondenz gefunden wird, wird die eingegebene Identifizierungsinformation mit einem zweiten Codierschlüssel codiert, der derselbe sein kann wie der erste Schlüssel. Die codierte Identifizierungsinformation wird mit veränderlicher Information wie z. B. der laufenden Transaktionsnummer oder des Geldbetrages kombiniert, um die wiederholte Übertragung identischer Verschlüsselungsfelder zu vermeiden und dann wieder mit einem dritten Übertragungsschlüssel codiert. Durch diesen Codierprozess braucht das Datenverarbeitungssystem nicht die Identifizierungszahl zu speichern sondern nur die verschlüsselte Identifizierungszahl. Die Datenbasis ist somit gegen ein betrügerisches Aufrufen der Korrospondenzliste zwischen Kontonummern und Identifizierungsnummern geschützt, aus der man gefälschte Karten zusammenstel-

len kann. Die verschlüsselte Identifizierungsinformation wird mit der Klartextanforderung und der Kreditkarteninformation kombiniert und dann dem Datenverarbeitungssystem mitgeteilt. Eine dreiteilige Transaktionsausführungsfolge beginnt mit einer Transaktionsanforderungsnachricht, die dem Datenverarbeitungssystem die verschlüsselte Identifzierungszahl, die mit veränderlichen Daten kombiniert und neu verschlüsselt wird, die Kreditkarteninformation und die durch die Tastatur eingegebene Transaktionsanforderungsinformation gibt. Der Benutzer kann z. B. die Auszahlung von 100 DM von einem Kreditkartenkonto verlangen. Bei Empfang einer Anforderung prüft das Datenverarbeitungssystem die Entsprechung zwischen der übertragenen codierten Identifierungszahl und der in der Datenbasis gespeicherten codierten Identifizierungszahl, Kontobeschränkungen sowie die Kreditobergrenze und wenn alles in Ordnung ist, sendet es eine Antwortnachricht, die die Transaktion genehmigt. Wenn nicht alles in Ordnung ist, lehnt das Datenverarbeitungssystem die geforderte Transaktion ab.

Genauso wie die Anforderungsnachricht enthält die nachfolgende Antwortnachricht einen verschlüsselten Teil, der ein Aktionskommando und veränderliche Daten enthält wie beispielsweise Geldbetrag oder eine Transaktionsnummer. Nachdem die codierte Information mit Klartextinformation wie beispielsweise einer Transaktionsbestätigungsinformation und einer Bildanzeigeinformation kombiniert ist, wird die Antwortnachricht an die anfordernde Station gesendet.

Bei Empfang der Antwortnachricht durch die die Transaktion anfordernde Station entschlüsselt die Station die Nachricht, prüft die Genauigkeit der veränderlichen Daten, um sich vor Fehlern zu schützen und führt dann die befohlenen Aktionen aus. Die Station erzeugt dann eine Zustandsnachricht um dem Datenverarbeitungssystem die Ausführung oder Annulierung der Transaktion und eventuelle Fehlerbedingungen an der Station mitzuteilen. Der verschlüsselte Teil der Zustandsnachricht enthält die Transaktionszahl, die Anzahl von Zustandbytes in der Nachricht und den Barbetragsstand.

Das Datenverarbeitungssystem antwortet durch Berechnung der angegebenen Transaktion oder Aufzeichnung der Transaktion oder Fortschreibung der Datenbasis auf den neuesten Stand. Wenn eine Fehlerbedingung angezeigt wird, kann das Datenverarbeitungssystem eine Befehlsnachricht senden und versuchen, den Fehler zu berichtigen oder die Station zu schließen, wenn der Fehler nicht behoben werden kann.

Durch diese Datennachrichtentechnik ist ein Verschlüsselungscode sehr schwer zu knacken und durch die Kommunikationsredundanz wird sichergestellt, daß das Datenverarbeitungssystem und eine Station auf richtige Nachrichten reagieren. Außerdem ist die Entsprechung zwischen der persönlichen Identifizierungszahl und der Kontonummer geschützt durch ein Verschlüsselungsschema, bei dem beide Zahlen in der Datenbasis nicht gespeichert zu werden brauchen.

Andere vorteilhafte Ausbildungen des Erfindungsgegenstandes sind den Unteransprüchen zu entnehmen.

Ein Ausführungsbeispiel der Erfindung ist in den Zeichnungen dargestellt und wird anschließend näher beschrieben. Es zeigen:

Fig. 1 in einem Funktionsblockdiagramm ein Transaktionsausführungssystem,

Fig. 2 in einem Funktionsblockdiagramm eine in dem in Fig. 1 gezeigten System benutzte Transaktionsstation (Terminal),

Fig. 3 in einem Operationsblockdiagramm die Anfangsverarbeitung der durch einen Benutzer eingeleiteten Transaktionsanforderung durch eine Transaktionsstation,

Fig. 4 in einem Operationsblockdiagramm die Verarbeitung empfangener Transaktionsanforderungen durch ein Datenverabeitungssystem und

Fig. 5 in einem Operationsblockdiagramm die Verarbeitung der Transaktionsantwortnachricht von einem Verarbeitungssystem durch eine Transaktionsstation.

Ein Transaktionsausführungssystem 10 enthält nach dem Erfindungsgedanken ein Datenverarbeitungssystem 12 und mehrere damit verbundene Transaktionsstationen 14. Das Datenverarbeitungssystem 12 besteht aus einer Zentraleinheit 16, einem Kommunikationssteuergerät 18 und einer Datenbasis, die Magnetbandeinheiten und Magnetplatteneinheiten umfassen kann. Die Zentraleinheit führt die zur Steuerung der Operation des Datenverarbeitungssystems 12 und zur Verarbeitung der durch das Kommunikationssteuergerät 18 empfangenen oder in der Datenbasis 20 gespeicherten Information notwendigen arithmetischen und logischen Operationen aus. Die Datenbasis 20 speichert Information über jeden Kunden des zentralen Verarbeitungssystems 12. Für einen Bankkunden kann die Datenbasis z. B. Kontoinformation über Kreditkarten, Sparkonten, Schecks oder andere Konten der Bank sowie Lohnlisteninformation und Information über den finanziellen Stand der Bankoperationen speichern. Jedes Konto kann in typischer Weise adressierbar sein nach einer Kontonummer und darin die laufende Kontoinformation gespeichert haben wie über den laufenden Kontostand, die Kontovorgänge für einen bestimmten Zeitraum, codierte persönliche Identifizierungsnummern für Personen, die zur Benutzung des Kontos berechtigt sind, eine oberste Kreditgrenze und andere Informationen, die die Bank als Teil eines Kontos speichern will. Das Kommunikationssteuergerät 18 wirkt als Schnittstelle zwischen der Zentraleinheit 16 und mehreren Kommunikationskanälen 20. Das Steuergerät 18 bringt durch die Zentraleinheit 16 empfangene Information in eine Kommunikationsdisziplin und hält die Synchronisation der Kommunikation aufrecht.

Eine Transaktionsstation 14 kann zur Kommunikation mit dem Datenverarbeitungssystem 12 in einer fast unbegrenzten Anzahl von Arten verbunden werden, wobei die verschiedenen in Fig. 1 gezeigten Methoden nur Beispiele sind. Eine Station kann z. B. direkt an das

Kommunikationssteuergerät 18 angeschlossen werden entweder durch eine lokale Kommunikationsverbindung wie das Kabel 24 für die lokale Benutzerstation 26 oder eine Funkverbindung 28 für eine entfernt stehende Benutzerstation 30. Andererseits kann eine Station aber auch an das Datenverarbeitungssystem 12 durch ein Steuergerät 32 angeschlossen werden wie z. B. das Gerät IBM 3601 entweder durch direkte Verbindung mit dem Steuergerät 32 durch das Kabel 34 für die Station 36 oder durch Verbindung mit einer Kommunikationsschleife 38. Obwohl andere Geräte in die Schleife eingeschlossen werden können, ist die Kommunikationsschleife 38 als Beispiel mit einer ersten Schalterarbeitsmaschine 40, einer zweiten Schalterarbeitsmaschine 42, einer ersten Benutzerstation 44 und einer zweiten Benutzerstation 46 dargestellt. Während die Kommunikationsschleife 38 Fernübertragungsverbindungen wie die Funkkommunikation oder die Kommunikation über öffentliche Leitungen für ein Banksystem enthalten kann, kann das Steuergerät 32 typischerweise in einer Zweigstelle der Bankt stehen, wobei alle Datenverarbeitungsstationen in der Zweigstelle in die Schleife 38 geschaltet sind. Das Steuergerät selbst kann an einen Kommunikationskanal 22 des Kommunikationssteuergerätes 18 entweder direkt durch eine Kommunikationsverbindung 48 wie die in Fig. 1 dargestellte öffentliche Leitung oder an eine Kommunikationsschleife 38 angeschlossen sein, die zu einem Kommunikationskanal 22 des Kommunikationssteuergerätes 18 läuft.

Im allgemeinen wirkt das Steuergerät 32 lediglich als Relaisstation für die Information, die durch die Schleife 38 geleitet wird, kann aber auch als Datenverarbeitungssystem dienen, wenn direkte Echtzeitkommunikation mit dem Datenverarbeitungssystem 12 nicht betrieben wird. Bei der Benutzung als Datenverarbeitungssystem muß das Steuergerät die Transaktionsausführungsinformation zur späteren Verarbeitung durch das System 12 speichern und Unterstützungsfunktionen liefern, die für den Betrieb einer Transaktionsstation 14 gebraucht werden.

In Fig. 2 ist ein Ausführungsbeispiel der Transaktionsstation 14 gezeigt, obwohl deren praktische Ausführung für die Erfindung nicht kritisch ist. Die Datenstation 14 ist im allgemeinen modular aufgebaut und enthält einen programmierbaren Mikroprozessor 60, der mit mehreren Stationsuntersystemen durch eine Informationssammelleitung 62 gekoppelt ist. Der Mikroprozessor 60 wird durch ein Taktsignal vom Taktsignalgenerator 64 gespeist und ist operativ an ein Datenspeichermodul 66 angeschlossen, welches sowohl den elektrisch veränderlichen Randomspeicher (RAM) als auch den Festwertspeicher (ROS) enthält. Der Festwertspeicherteil des Datenspeichers 66 speichert die verschiedenen Operationsprogramme für den Mikroprozessor 60 und der Randomspeicherteil liefert den Arbeitsbereich für die Programmausführung. Bei typischen in integrierter Schaltung ausgeführten Speichern geht der Inhalt des Randomspeichers bei Stromausfall verloren.

STATIONSINFORMATIONSSAMMELLEITUNG

Der Mikroprozessor 60 steht mit den Untersystemen lediglich durch die Stationsinformationssammelleitung 62 in Verbindung. Diese Verbindungstechnik mit dem Mikroprozessor 60 über die Sammelleitung 62 gestattet dem Mikroprozessor 60 den Empfang detaillierter Information über den Stationszustand und die detaillierte Lenkung der Stationsmaschinenoperationen ohne größere Informationseingabe- und Ausgabeverbindungen. Die Stationszustandsinformation wird von den einzelnen Stationsuntersystemen abgefühlt. Diese Information wird dann auf Befehl vom Mikroprozessor 60 an diesen übertragen. Ähnlich ist in den Untersystemmodulen die Treiberschaltung und die Maschinenausrüstung für die Ausführung von Mikroprozessorbefehlen enthalten. Die Mikroprozessorbefehle sind extreme Grundbefehle und in ihrer Art detailliert. Jeder Befehl führt eine Grundoperation im Untersystem aus wie z. B. das Ein- oder Ausschalten eines Motors, die Bildanzeige oder den Druck eines Zeichens, den Transport einer Rechnung oder das Lesen eines Kommunikationszeichens. Die Informationssammelleitung 62 führt ein Systemrückstellsignal, neun Dateneingangssignale (8 Bits + Parität) zur Übertragung von Information an den Prozessor 60, neun

Datenausgangssignale (8 Bits + Parität) zur Übertragung von Information vom Mikroprozessor 60 an ein angeschlossenes betriebsbereites Untersystem und Sammelleitungssteuersignale zur Steuerung der Informationsübertragung auf der Sammelleitung 62.

UNTERSYSTEM ZUR PROZESSORUNTERSTÜTZUNG

Über die Sammelleitung 62 ist ein Prozessorunterstützungssystem 68 an den Mikroprozessor 60 angeschlossen. Das Prozessorunterstützungssystem 68 gibt dem Mikroprozessor 60 maschinelle Unterstützung im Gegensatz zu den anderen Stationsuntersystemen, die mit bestimmten Gesichtspunkten des Betriebes der Transaktionsstation 14 zusammenhängende Funktionen haben.

Das Prozessorunterstützungssystem 68 empfängt ein Taktsignal von 1MHz vom Taktsignalgenerator 64 und teilt dieses Signal zur Erzeugung von Taktsignalen mit niedrigerer Frequenz, die in anderen Untersystemen benutzt werden. Ein Taktsignal mit niedrigerer Frequenz wird für die Erzeugung der periodischen Unterbrechungskommandos in Intervallen von 10 ms benutzt. Diese Unterbrechungskommandos lösen eine Unterbrechungslogik im Prozessorunterstützungssystem 68 aus, um den Mikroprozessor alle 10 ms zu unterbrechen. Der Mikroprozessor 60 benutzt diese Taktunterbrechungsperiode, um eine Zeitbasis zur Vorgangssteuerung für die verschiedenen Operationen an der Transaktionsstation 14 zu haben. Eine Rückstellogik im Unterstützungssystem 68 steuert die Rückstelleitung der Informationssammelleitung 62. Wenn diese Rückstelleitung erregt ist, wird der Prozessor 60 sowie alle an die Sammelleitung 62 angeschlossenen Modulen initialisiert und jede ausstehende Benutzertransaktion gelöscht. Der Prozessor 60 wird in eine vorgegebene Programminstruktion zurückgeführt, von wo die Programmausführung nach der Rückstellung wieder aufgenommen werden kann. Das Rückstellsignal wird aufgrund der Wechselstromeinschaltung, eines Signales vom Rückstellschalter oder eines Hängesignales vom Hängedetektor im Unterstützungssystem 68 erregt. Der Hängedetektor überwacht die Steuerleitungen der Sammelleitung 62 und

erzeugt ein Hängesignal, wenn die Aktivität auf der Sammelleitung für einen Zeitabschnitt aufhört, der lang genug ist um anzuzeigen, daß der Mikroprozessor 60 nicht richtig arbeitet. Ein Laufdetektor reagiert auf die Unterbrechungsanforderungssignale des Taktgebers und erzeugt ein Laufsignal, welches so lange hochgehalten wird, wie der Mikroprozessor regelmäßig auf die Anforderungen antwortet. Wenn eine vorgegebene Periode abläuft, ohne daß eine Zeitgeberunterbrechungsanforderung verarbeitet wurde, beendet der Laufdekektor das Laufsignal. Das Prozessorunterstützungssystem 68 enthält auch eine Datenleselogik, die eine Reihe serieller Information, wie sie von einer Benutzerkreditkarte gelesen wird, empfängt, die Daten - von der Taktinformation trennt, den binären Bitstrom parallel umsetzt und die Sammelleitung 62 zur Verarbeitung durch den Mikroprozessor 60 gibt.

MECHANISCHES STEUER-UNTERSYSTEM

Ein mechanisches Steuer-Untersystem 70 liefert die eigentliche mechanische Manipulation verschiedener maschineller Einrichtungen der Transaktionsstation 14. Das Untersystem 70, welches wie die anderen Untersysteme keinerlei Verzweigungs- oder Entscheidungsmöglichkeit hat, führt elementare Grundkommandos vom Mikroprozessor 60 aus und sammelt Information über den physikalischen Zustand der verschiedenen Maschinenfunktionen zur Rückmeldung an den Mikroprozessor 60. Als Beispiel für die einzelnen Elementarfunktionen, die von dem mechanischen Steuer-Untersystem 70 ausgeführt werden können, sei eine Kreditkartenverarbeitungseinrichtung genannt, die auf Richtungs- und Bewegungskommandos für die Kreditkarten reagiert und einen Motor schaltet, der ein Kartentransportsystem so treibt, daß die Kreditkarte unter einen Lesekopf bewegt wird. Fühler (Schalter oder Photozellen) sind so eingestellt, daß das Vorhandensein der Kreditkarte am Eingang (1), am Ausgangsverklemmungsfühler (2) und in den Kartenübertragungspositionen (3) abgefühlt wird. Wenn ein Fühler betätigt wird, steht ein Informationsbit in einem Statuswort zur

Verfügung, welches diesen Zustand anzeigt. Wenn der Mikroprozessor 60 die verschiedenen Statuswörter während einer Leseoperation periodisch liest, stellt er fest, daß die Kreditkarte den Übertragungsbereich erreicht hat, wo sie festgehalten wird. Der Mikroprozessor 60 befiehlt dann die Umkehrung der Drehrichtung des Kreditkartentransportmotors für eine kurze Zeit, um "zu trennen" und befiehlt dann die Abschaltung des Motors. In ähnlicher Weise kontrolliert das mechanische Steueruntersystem 70 die komplette Verarbeitung der Kreditkarte sowie den Einzug oder die Rückgabe an den Benutzer. Zu den weiteren Funktionen des Untersystems gehört die Kontrolle der Depositen, wo der Benutzer Unterlagen deponieren kann, die in einen Aufbewahrungsbehälter so geleitet werden, daß der Benutzer niemals Zugang zum Behälter hat. In ähnlicher Weise kann das mechanische Untersystem 70 das Öffnen und Schließen von Benutzerzugangstüren und die Ausgabe vorbestimmter Bargeldbeträge an einen Übertragungsbereich steuern, wo auch gedruckte Transaktionsbeläge gesammelt werden können zusammen mit dem Bargeld und der Ausgabe oder dem Einzug von Belegen, die im Übertragungsbereich vorgelegt wurden. Das mechanische Kontrolluntersystem 70 fühlt aber nicht nur den Zustand der mechanischen Maschinenausrüstung ab sondern auch das Vorhandensein des durch die Bargeldausgabeanlage gespeicherten Bargeldes und zeigt an, wenn nicht genügend Bargeld zur Verfügung steht, um eine Transaktion mit dem Ausgabehöchstwert vorzunehmen. Außerdem fühlt das System verschiedene Zustände ab, die einer entfernt stehenden Bedientafel sowie dem Prozessor 60 mitgeteilt werden können. Zu diesen Fernsignalen gehört eine Anzeige dafür, ob die Bedienungstür geöffnet ist, ob ein Eindringschutzgitter gestört wurde und ob ein Eingreifen erforderlich ist oder nicht. Außerdem können an die Fernbedientafel noch Signale über Transaktionsbestätigungen oder über niedrigen Bargeldbestand, die Öffnung der Bediener-Zugangstür sowie die Kommunikationsbereitschaft zwischen der Station und dem Datenverarbeitungssystem übertragen werden. Zu den Kommandoschaltern an der Fernbedientafel gehören ein Stationsrückstellschalter und ein Schalter, der die Überprüfung der Kommunikationsverbindung befiehlt.

BENUTZER-KOMMUNIKATIONSSYSTEM

Ein Benutzer-Kommunikationssystem 72 steuert die bidirektionale Kommunikation zwischen der Transaktionsstation 14 und einem Benutzer. Das Kommunikationssystem 72 enthält eine Tastatur Aufnahme der vom Benutzer erzeugten Befehle, ein Bildanzeigegerät mit 222 horizontalen Punkten mal 7 Punkten und eine Steuerlogik sowie einen Wiederholungspuffer für dieses Bildanzeigegerät. Die Bildanzeigesteuerlogik empfängt das "Punktbild" der jeweiligen Anzeige und setzt diese Bildanzeige dann fort, bis ein gegenteiliges Kommando empfangen wird.

Die Tastatur ist in mehrere Felder unterteilt, von denen jedes eine Anzahl von Tasten enthält. Ein Transaktionswahlfeld zeigt z. B. die Art der Transaktion an, die ein Benutzer ausführen will. Andere Felder enthalten ein Kontoabgangswahlfeld, welches ein Konto anzeigt, von dem Beträge zu nehmen sind, ein Kontozugangswahlfeld, welches ein Konto anzeigt, auf das Beträge zu deponieren sind sowie ein numerisches Tastaturfeld, welches die Eingabe von Dezimalzahlen wie beispielsweise der persönlichen Identifizierungszahl oder von Dollarbeträgen gestattet. "Rückwärtslampen" sind auf den Funktionswahltasten, den Kontozugangstasten und den Kontoabgangstasten vorgesehen und erzeugen eine Anzeige, auf der der Benutzer verfolgen kann, welche Tasten auf den vorher benutzen Feldern gewählt wurden. Alle Rückwärtslampen leuchten in dem Feld auf, in dem die nächste Tastenbetätigung erfolgen sollte. Wenn z. B. ein Benutzer seine Kreditkarte in die Transaktionsstation 14 einlegt, wird er aufgefordert, seine persönliche Identifizierungszahl einzutasten. Nach richtigem Empfang dieser Zahl würden alle Tasten im Funktionswahlfeld aufleuchten. Wenn der Benutzer eine bestimmte Taste wie beispielsweise die Betragsübertragungstaste betätigt, verlöschen alle anderen Rückwärtslampen und nur die Betragsübertragungstaste leuchtet weiter. Alle Tasten im nächsten Feld, beispielsweise dem Kontoabgangsfeld, leuchten dann auf um den nächste Schritt bei der Transaktionsanforderung vorzubereiten. Auf diese Weise könne über die Anzeige früherer Wahlvorgänge verfolgt und das nächste Wahlfeld bezeichnet werden.

Mit Bildanzeigenachrichten und Farbcodierung kann man den Benutzer in der richtigen Reihenfolge anleiten. Die Tastatursteuerlogik des Benutzerkommunikationssystems 72 enthält die Schaltung, die zur Rückleuchung bestimmter Tasten auf Kommando des Mikroprozessors 60 und zur Anzeige an den Mikroprozessor, welche Tasten vom Benutzer betätigt wurden, notwendig ist.

TRANSAKTIONS-BELEGGEBER

Ein Transaktions-Beleggebersystem 74 enthält einen Formularbehandler zum Transport der Transaktions-Belegsformulare, einen Drucker, eine Druckersteuerlogik und eine Logik zum Anschalten dieses Untersystemes 74 an die Sammelleitung 62. Der Transaktions-Beleggeber 74 führt nur bestimmte Grundkommandos aus wie das Starten der Bewegung oder das Drucker bestimmter Zeichen. Das Untersystem 74 sammelt Information über den physikalischen Zustand der Maschinenausrüstung im Transaktions-Beleggeber zur Mitteilung über die Sammelleitung 62 an den Mikroprozessor 60. Mit dieser Information erkennt der unter Programmsteuerung laufende Mikroprozessor dann den erfolgreichen Abschluß einer bestimmten Elementarfunktion und befiehlt die Einleitung weiterer Funktionen.

BEDIENER-FUNKTIONSUNTERSYSTEM

Ein Bediener-Funktionsuntersystem 76 bietet der Bedienungskraft Wartungsanschlüsse und enthält Eingabeschalter, eine vierstellige Hexadezimal Bildanzeige, eine Stromfühlerschaltung, einen gegen Stromausfall geschützten 128 Byte großen Zusatzspeicher, der zum Speichern von Systemparametern benutzt wird, und ein Verzeichnis von Ausnahmeinformation. Zu den gespeicherten Parametern gehören eine Betragszählerzahl, Codierschlüssel und eine Transaktionszahl. Die Bedienertafel wird zugänglich durch eine doppelt verriegelte Tür an der Rückseite der Station 14, die zum Betrieb der Station durch den Benutzer geschlossen sein muß. Öffnet man die zugangstür und versucht eine Wartungsfunktion, so werden dadurch

die Codierschlüssel zerstört, die normalerweise in diesem Zusatzspeicher stehen. Diese Zerstörung der Schlüssel schützt die Schlüssel vor einem Bediener, der eventuell versucht, mit elektronischen Instrumenten den Schlüssel aus dem nichtflüchtigen Speicher zu lesen. Die Schlüssel müssen dann über die Tastatur von einer stark vertrauenswürdigen Person neu eingegeben werden, bevor die Station wieder geöffnet werden kann. Die 8 Byte großen Schlüssel werden jeweils in Form von 16 hexadezimal Zahlen in Gruppen von je zwei Zahlen eingegeben. Um die Schwierigkeit bei der verbotenen Entdeckung der Schlüssel zu erhöhen, werden bei der Eingabe der Schlüssel nur die beiden jeweils vorhergehenden Zahlen angezeigt. Andererseits kann ein Schlüssel A, der die Korrospondenz zwischen Kontonummern und persönlicher Identifizierungszahl definiert, nocht weiter geschützt werden, indem die Eingabe des entzifferten Schlüssels A (Schlüssel A') verlangt wird, der dann nach einem vierten Verschlüsselungssystem codiert wird um den tatsächlichen Schlüssen A zu erzeugen. Mit dieser Technik kann der eigentliche Schlüssel A am Ort der Transaktionsstation 14 vor allen Personen geschützt bleiben. Die Stromfühlerschaltung überwacht sowohl die Netzwechselspannung als auch die internen Gleichstrompegel und bei Verlustanzeige der Wechselspannung und niedrigen aber noch nutzbaren Gleichspannungen wird an den Mikroprozessor 60 ein Signal zur Rettung kritischer Information gesendet und dann wird der Zugang zum Zusatzspeicher beschränkt, während der Speicher von der Hilfsstromquelle versorgt wird. An die Bedienertafel wird so lange ein Anzeigesignal gegeben, wie die logischen Gleichspannungen ausreichend sind.

KOMMUNIKATIONSUNTERSYSTEM

Ein Kommunikationsuntersystem 78 sorgt für die Kommunikationsverbindung zwischen einem Kommunikationskanal und der Informationssammelleitung 62. Das Kommunikationsuntersystem 78 ist ein konventionelles System und empfängt byteweise Information von der Sammelleitung 62 oder gibt Information für die Datenstation an dieser Leitung.

FERNANSCHLUSS

Ein Fernsignalstecker 82 gestattet den Anschluß einiger Zustandssignaleingänge und einiger Steuersignaleingänge an eine Fernbedientafel, die eigentlich Teil der Station 14 ist. Eine Bankzweigstelle kann z. B. Transaktionsstationen 14 und eine zentrale Fernsteuertafel mit optischer Bildanzeige und Steuerschaltern für jede der 5 Transaktionsstationen 14 an einer passenden zentralen Stelle haben. Diese Fernsignale dienen primär der Überwachung des Stationsbetriebes oder der Steuerung von Sondenzuständen und werden für die normale Benutzertransaktion nicht benutzt. Die einzelne Fernsteuertafel wurde vorher schon erklärt.

KOMMUNIKATIONSNACHRICHTENFORMAT

Es gibt im wesentlichen zwei verschiedene Arten von Nachrichten, die von einer Transaktionsstation 14 an ein Datenverarbeitungssystem gesendet werden können und vier Arten von Nachrichten, die vom Datenverarbeitungssystem 12 an eine Transaktionsstation 14 gesendet werden können. Die Nachrichten von der Station zum System enthalten eine Transaktionsanforderungsnachricht, die normalerweise die erste Kommunikationsnachricht ist, der eine vom Benutzer eingeleitete Transaktions- und eine Zustands. nachricht folgen, die typischerweise die letzte der drei Nachrichten in dieser Folge ist. Es gibt zwei Grundtypen von Zustandsnachrichten. Die erste Nachricht ist eine Zustandsantwortnachricht, die als dritte Kommunikationsnachricht in einer normalen Benutzer-Transaktionsfolge dient und dem Datenverarbeitungssystem den Abschluß oder die Annulierung einer vom Benutzer angeforderten Transaktion mitteilt. Die zweite Nachrichtenart ist eine Ausnahmezustandsnachricht, die einen Zustand oder eine Bedingung für eine Station 14 anzeigt, die außerhalb der normalen Betriebsbedingungen liegt. Eine Ausnahmezustandsnachricht würde z. B. aufgrund eines Anfragebefehles vom Datenverarbeitungssystem gesendet, wenn die Wartungstür geöffnet ist, bei Erkennen einer schweren Fehlerbe-

dingung wie beispielsweise einer Verklemmung der Benutzertür oder eines schweren Maschinenfehlers oder wenn eine Zeitinitialisierung benötigt wird.

Vom Datenverarbeitungssystem 12 können an die Transaktionsstation 14 vier Arten von Nachrichten übertragen werden, und zwar eine Transaktionsantwortnachricht, eine Befehlsnachricht, eine Lade-Initialisierungsnachricht und eine Echonachricht. Die Transaktionsantwortnachricht ist die normale Antwort auf eine Transaktionsanforderungsnachricht im Laufe einer normalen Benutzertransaktion und teilt der Transaktionsstation 14 die Art mit, in der die angeforderte Transaktion auszuführen ist. Eine Befehlsnachricht befiehlt Änderungen im logischen Zustand einer Station 14 und kann auch als Anfrage für eine Zustandsnachricht dienen, wenn keine Änderungen gewünscht werden. Eine Lade-Initialisierungsnachricht wird von einem Datenverarbeitungssystem an eine Station 14 als Antwort auf eine Ausnahmezustandsnachricht gesendet, die die Initialisierung anfordert (IPNL). Die Ladeinitialisierungsnachricht enthält Nachrichtentext, eine Zusatzauswahlinformation, Fonttabellen, Programmroutinen und Dateninformation zur Speicherung im flüchtigen Randomteil des Datenspeichers 66 des Mikroprozessors 60 innerhalb der Transaktionsstation 14. Mit einer Echonachricht wird eine Fehlersuchbestätigungsprüfung durchgeführt und sie kann nur gesendet werden, wenn sich eine Transaktionsstation 14 im geschlossenen Zustand befindet. Die Station 14 antwortet auf eine Echonachricht mit einer Echonachricht.

Für die Kommunikation von Nachrichten zwischen einer Transaktionsstation 14 und einem Datenverarbeitungssystem 12 kommen nur drei Grundnachrichtenfolgen in Frage. Eine Einzelnachrichtenfolge besteht aus einer Ausnahmezustandsnachricht, die vo einer Station 14 an ein Datenverarbeitungssystem 12 gesendet wird. Diese kann entweder das Auftreten eines abnormalen Zustandes anzeigen oder eine Initialisierungsanforderung sein. Eine Befehlsnachricht vom Datenverarbeitungssystem ist nicht erforderlich. Der Nachrichteninhalt bezeichnet den Fall.

Eine Folge aus zwei Nachrichten kann entweder eine Kommandonachricht vom Datenverarbeitungssystem, eine Ladeinitialisierungsnachricht vom Verarbeitungssystem 12 an die Station 14 enthalten, der eine entsprechende Zustandsnachricht von der Station 14 an das Datenverarbeitungssystem 12 folgt oder eine Echonachricht vom Datenverarbeitungssystem, der eine Echonachricht von der Station folgt. Die Transaktionsstation 14 weist ein Kommando zurück, welches empfangen wird, während die Station einen vorhergehenden Befehl, eine nicht erkennbare Nachricht oder eine nicht angeforderte Transaktionsantwortnachricht verarbeitet. In jedem Fall kann das Datenverarbeitungssystem entweder ein entferntstehendes oder ein direkt örtlich angeschlossenes System sein.

Jedesmal wenn die Transaktionsstation 14 den Stromeinschaltzustand annimmt, muß sie eine Ladeinitialisierungsnachricht anfordern und vom Datenverarbeitungssystem empfangen, bevor sie zur Annahme von Transaktionen wieder geöffnet werden kann. Die Transaktionsstationen 36, 44 und 46 in Fig. 1 sind an ein Steuergerät 32 angeschlossen und können unabhängig arbeiten. Unter solchen Umständen dient das Steuergerät 32 als Datenverarbeitungssystem und verzeichnet lediglich die Benutzertransaktionen beispielsweise auf einem Magnetband oder einer Platte. Die Transaktionsinformation wird dann einem Buchungssystem zu einem späteren Zeitpunkt zur Verfügung gestellt, damit die Konten auf den neuesten Stand gebracht werden können. Beim abhängigen Betrieb können einige Funktionen der Datenverarbeitunsanlage durch das Steuergerät 32 wahrgenommen werden wie beipielsweise die Speicherung des Initialisierungsprogrammes für die Stationen, normalerweise laufen aber alle Kommunikationen unverändert zum Datenverarbeitungssystem 12. In einem solchen abhängigen Betrieb muß das Datenverarbeitungssystem 12 die in seiner Datenbasis gespeicherten Kontenbestände in Echtzeit auf den neuesten Stand bringen, d. h. sobald die vom Benutzer angeforderten Transaktionen ausgeführt werden.

Jedesmal wenn die Stromversorgung an der Transaktionsstation 14 verlorengeht, geht auch Information aus dem RAM-Teil des Datenspeichers 66 verloren und beim Wiedereinschalten des Stromes muß die Initialisierung angefordert werden. Nach Empfang der Initialisierungsinformation vom Datenverarbeitungssystem kann eine Transaktionsstation 14 zum Empfang von Benutzertransaktionen geöffnet werden, jedoch nur auf Befehl von der Datenverarbeitungsanlage her. Die Initialisierung erfolgt durch eine Transaktionsstation 14 durch Senden einer die Initialisierung anfordernden Ausnahmezustandsnachricht im Einzelnachrichtenformat. Die Datenverarbeitungsanlage leitet dann eine neue Kommunikationsfolge ein, indem sie eine Initialisierungsnachricht (in mehreren Teilen) sendet, die die angeforderte Initialsierungsinformation enthält. Beim erfolgreichen Empfang der Initialisierungsinformation führt die anfordernde Station 14 die zweiteilige Nachrichtenfolge zu Ende durch Rücksendung einer Zustandsnachricht an das Datenverarbeitungssystem.

Jede zwischen einer Transaktionsstation 14 und einem Datenverarbeitungssystem 12 gesendete Nachricht, beginnt mit einem 4 Byte großen Vorlauffeld. Byte 1 des Vorlauffeldes ist ein Nachrichtenlängenbyte (L), welches die binäre Anzahl von Nachrichtenbytes im Nachrichtentext (einschließlich L) enthält. Byte 2 ist eine 1 Byte große Transaktions-Reihenfolgezahl (N) in binärer Form. Diese Zahl wird für jede neue Benutzertransaktion erhöht und ist in allen für diese Transaktion ausgetauschten Nachrichten enthalten. Die Zahl hat einen Bereich von 1 bis einschließlich 255. Null (hex 00) wird für Nachrichten verwendet, die nichts mit einer Benutzertransaktion zu tun haben. Somit läuft ein Transaktionszähler, der für jede neue Benutzertransaktion erhöht wird, von Hexadezimal FF über nach Hexadezimal 01. Die Transaktionszahl (N) wird in dem gegen Stromausfall geschützten Zusatzspeicher des Bedienerfunktionssystems 76 gespeichert, so daß sie nach einem kurzzeitigen Stromausfall verfügbar bleibt. Byte 3 des allgemeinen Vorlauffeldes ist ein Klassenbyte (C), welches die Art der gesendeten Nachricht und somit ihr Format identifiziert. Byte 4, das letzte Byte des Vorlauffeldes, bezeichnet eine Nachrichtenunter-

klasse (SC), die als Modifizierer für das Nachrichtenklassenbyte dient.

Eigentlich sind nur einige wenige Kombinationen von Nachrichtenklassen (C) und Unterklassen (SC) implementiert. Die Klasse Hexadezimal 01 bezeichnet eine Transaktionsanforderungsnachricht von einer Transaktionsstation 14 an ein Datenverarbeitungssystem. In der Klasse 01 wurden neun Unterklassen implementiert. Die Unterklasse Hexadezimal 00 gibt an, daß eine vom Benutzer angeforderte Transaktion nicht abgeschlossen ist, weil die Identifizierungszahl nicht richtig eingegeben wurde. Die Unterklasse Hexadezimal 01 bezeichnet eine Bargeldausgabeanforderung. Die Unterklasse Hexadezimal 02 bezeichnet eine Kontoanfrage. Die Unterklasse Hexadezimal 03 besagt, daß ein Benutzer Beträge deponieren will. Die Unterklasse Hexadezimal 04 besagt, daß ein Benutzer Beträge von einem Konto auf ein anderes übertragen will. Die Unterklasse Hexadezimal 05 besagt, daß ein Benutzer eine Rechnung oder Leistung bezahlen will durch Deponieren von Geld in der Transaktionsstation. Die Unterklasse Hexadezimal 05 zeigt eine besondere Transaktion an, deren Art durch Eingabe einer vorbestimmten Zahl über die Tastatur und nicht durch Betätigen einer Taste im Transaktionswahlfeld der Tastatur identifiziert wird. Die Unterklasse Hexadezimal 07 zeigt an, daß eine geforderte Transaktion unvollständig ist, weil die Depositenklappe, die den Depositenbehälter abdeckt, gewaltsam geöffnet wurde. Die Unterklasse Hexadezimal 08 bezeichnet die Anforderung eines Benutzers, eine Rechnung zu bezahlen durch Übertragen von Beträgen von einem Konto zum anderen.

Eine Nachrichtenklasse mit der Bezeichnung C = Hexadezimal 15 bezeichnet eine Zustandsnachricht von einer Station 14 an ein Datenverarbeitungssystem 12. In dieser Klasse gibt es fünf Nachrichtenunterklassen. Die Unterklasse Hexadezimal 01 bezeichnet eine Transaktionsabschlußzustandsnachricht. Die Unterklasse Hexadezimal 02 besagt, daß die Nachricht eine Antwort auf die Ausführung eines Befehles ist und die Zustandszahl N im allgemeinen Vorlauf muß auf Null gesetzt werden. Die Unterklasse Hexadezimal

03 ist eine Ausnahmezustandsnachricht und zeigt eine Fehlerbedingung oder die Anforderung der Initialisierung an, und die Transaktionszahl N muß auf Null gesetzt werden. Die Unterklasse Hexadezimal 04 besagt, daß die Zustandsnachricht eine Antwort auf die Initialisierung ist und die Transaktionszahl N muß auf Null gesetzt werden. Die Unterklasse Hexadezimal 08 ist eine Wiederholungsanforderung oder eine Befehlsantwortnachricht und die Transaktionszahl N muß für diese Nachricht auf Null gesetzt werden. Eine Wiederholungsanforderung zeigt an, daß das Datenverarbeitungssystem die Spur der richtigen Transaktion verloren hat und auf den neuesten Stand gebracht werden muß. Die Transaktionsstation antwortet mit einer Ausnahmezustandsnachricht.

Eine Transaktionsantwortnachricht von einem Datenverarbeitungssystem an eine Transaktionsstation 14 wird bezeichnet durch die Klasse Hexadezimal OB. Durch das Unterklassenbyte in dieser Klasse werden neun Unterklassen bezeichnet. Die Unterklassenbezeichnung Hexadezimal 00 besagt, daß die Transaktion unvollständig ist, weil die Identifizierungsnummer nicht richtig eingegeben wurde. Die Unterklassenbezeichnung Hexadezimal 01 bezeichnet eine Transaktionsanforderung für Bargeldausgabe. Die Unterklassenbezeichnung Hexadezimal 02 bezeichnet eine Transaktionsanforderung für einen Kontoauszug. Die Unterklassenbezeichnung Hexadezimal 03 bezeichnet eine Depositionsanforderung. Die Unterklassenbezeichnung Hexadezimal 04 bezeichnet eine Betragsüberweisungsanforderung von einem Konto zum anderen. Die Unterklassenbezeichnung Hexadezimal 05 zeigt eine Transaktionsanforderung für die Bezahlung einer Rechnung an durch Überweisen von in der Station für ein Konto deponierten Beträgen. Die Unterklasse Hexadezimal 06 bezeichnet eine Transaktion mit einem Sonderwunsch, wobei die Art der Transaktion durch die über die numerische Tastatur eingetastete Zahl und nicht durch Betätigen einer Taste im Transaktionswahlfeld durch den Benutzer bestimmt wird. Die Unterklasse Hexadezimal 07 zeigt an, daß die Nachricht zu einer angeforderten Benutzertransaktion gehört, die unvollständig ist, weil die Depositenklappe der Station 14 mit Gewalt geöffnet wurde. Die Unterklasse Hexadezimal 08 bezeichnet eine Benutzertransaktion, in der eine Rechnung oder ein

Lohn zu zahlen ist durch Überweisung von Beträgen von einem Konto zum anderen.

Die Klasse Hexadezimal OC identifiziert eine Befehlsnachricht vom Datenverarbeitungssystem an eine Transaktionsstation 14. Eine Befehlsnachricht gehört nicht zu einer bestimmten Transaktion und daher wird die Transaktionszahl N des Vorlauffeldes immer auf Null gesetzt. Die Unterklasse Hexadezimal 01 bezeichnet einen Öffnungsbefehl, die Unterklasse Hexadezimal 02 einen Befehl zum Schließen der Transaktionsstation 14. Die Unterklasse Hexadezimal 03 bezeichnet eine Anfragenachricht, in der eine Transaktionsstation 14 keine Funktion aufgrund des Befehles ausführen kann sondern mit einer Zustandsnachricht anworten muß. Die Unterklasse Hexadezimal 04 bezeichnet eine Befehl zur Änderung des dritten Schlüssels (Schlüssel B), nämlich des Übertragungscodeschlüssels von dem vorliegenden Schlüssel auf einen in der Nachricht enthaltenen Schlüssel. Die Unterklasse 05 bezeichnet einen Befehl zum Setzen des Übertragungscodeschlüssels (Schlüssel B) unter Verwendung eines Reserveschlüssels (Schlüssel C). Die Unterklasse Hexadezimal 06 besagt, daß eine Transaktionsstation 15 beauftragt wird, eine Anfangsprogrammladung anzufordern. Die Unterklasse Hexadezimal 07 besagt, daß die Nachricht entweder ein Befehl zum Ändern der optischen Anzeige oder eine schriftliche Nachricht enthält, die durch den Transaktionsbeleggeber zu drucken ist. Die Unterklasse Hexadezimal 08 ist ein Befehl für die Transaktionsstation 14, an die Datenverarbeitungsanlage eine Wiederholungsanforderungsnachricht Klasse Hexadezimal 15 Unterklasse Hexadezimal 08 zurückzusenden.

Die Nachricht zum ersten Programmladen von der Datenverarbeitungsanlage an eine Transaktionsstation wird bezeichnet durch die Klasse Hexadezimal OD und hat nur eine Unterklasse mit der Bezeichnung Hexadezimal 01.

Eine Echonachricht vom Datenverarbeitungssystem an eine Station 14 wird durch die Klasse Hexadezimal 10 bezeichnet. In dieser Klasse gibt es vier Unterklassen von Echonachrichten. Die Unterklasse Hexadezimal 00 ist die Grundechonachricht und befiehlt der Transaktionsstation 14 lediglich, die Echonachricht an die Datenverarbeitungsanlage zurückzuübertragen. Die Unterklasse Hexadezimal 01 bezeichnet einen konservierten Echonachrichtenbefehl, der auf Bitmuster und Echo überprüft wird. Die Bytes der Daten im konservierten Text sind so angelegt, daß alle möglichen Bitmuster zur Prüfung der Arbeitsweise der Kommunikationseinrichtungen gesendet werden. Das Nachrichtenmuster wird durch die Station zum Vergleich mit einer zweiten Übertragung des Nachrichtenmusters zurückgehalten. Eine Unterklasse mit der hexadezimalen Bezeichnung 02 für eine Aufzeichnung mit veränderlichem Echo unterscheidet sich von der Unterklasse für das konservierte Echo nur dadurch, daß die Nachricht vom Datenverarbeitungssystem eingegebene Daten enthalten kann. Die Transaktionsstation gibt die Nachricht zurück und hält sie außerdem im Speicher zum Vergleich mit einer zweiten Übertragung derselben Nachricht fest. Bei Empfang der zweiten Übertragung der Nachricht prüft die Transaktionsstation und gibt die Nachricht zurück wie für die Unterklasse 01. Eine Datenverzeichnisanforderungsnachricht wird bezeichnet durch die Unterklasse 03. Die Station sendet daraufhin die acht neuesten Fehlerberichte. Eine Verschlüsselung oder Entschlüsselung ist von der Übertragung einer Echonachricht nicht betroffen.

Dem vier Byte großen Vorlauffeld einer jeden Nachricht folgen die Nachrichtendaten in einem Format, das von der Art der jeweils gesendeten Nachricht abhängt. Für eine Transaktionsanforderungsnachricht von der Station 14 zum Datenverarbeitungssystem folgt den allgemeinen Vorlaufbytes 1-4 ein 32 Bit großes verschlüsseltes Feld in den Bytes 5-8. Dieses 32 große verschlüsselte Feld wird später genauer beschrieben, allgemein kann jedoch gesagt werden, daß dieses Feld eine verschlüsselte Form der persönlichen Identifizierungsnummer enthält, die durch den Benutzer der Tasta-

tur eingegeben wurde, und ein Byte mit veränderlicher Information, die entweder der Inhalt eines Bargeldzählers oder eines Transaktionszahlenzählers sein kann.

Byte 9 ist ein Kontoabgangswahlbyte (FAS), welches angibt, welche Taste innerhalb des Kontoabgangswahlfeldes von der Benutzertastatur betätigt wurde. Der Dateninhalt dieses neunten Byte gibt die Art des Kontos an, von dem die Beträge für die vom Benutzer angeforderte Transaktion zu nehmen sind. Hexadezimal 21 bezeichnet ein Scheckkonto, Hexadezimal 22 ein Sparkonto, Hexadezimal 23 ein Kreditkartenkonto und Hexadezimal 24 ein Sonderkonto, welches durch einen Zahlenmodifizierer weiterdefiniert ist. Durch Sondervereinbarungen mit der Bank kann ein Benutzer mehrere Konten eröffnen. Diesen Konten kann dann eine vorbestimmte dreistellige Dezimalzahl zugeordnet werden. Durch Betätigen der Sonderwahltaste auf der Tastatur kann der Benutzer bis zu drei Dezimalzahlen durch die numerische Tastatur eingeben, um anzugeben, welches von möglicherweise vielen vorgegebenen Konten er belasten will. Diese Kontenbezeichnungszahl wird mit einer Stelle pro Byte und den Bytes 10-A übertragen, worin A die Werte 10, 11 oder 12 abhängig davon einnehmen kann, ob die über Sondertastatur bestimmte Kontonumer 1, 2 oder 3 Stellen hat. Da das FAS-Feld eine veränderliche Länge haben kann, muß ihm ein Feldtrennungsbyte (FS) mit dem Dateninhalt Hexadezimal FE folgen, wodurch die Grenzen des Feldes mit veränderlicher Länge definiert werden. Nebeneinanderliegende Feldtrenner bezeichnen eine Nullänge oder die Tatsache, daß zwischen ihnen keine Eintragung liegt. Das FS-Byte begrenzt das Ende des vorhergehenden Feldes.

Nach dem FS-Byte für das Kontoabgangswahlfeld (FAS) steht ein Kontowahlfeld (TAS), welches eine betätigte Taste innerhalb des Kontozugangsfeldes der Benutzertastatur bezeichnet. Hexadezimal 31 besagt, daß Beträge auf ein Scheckkonto deponiert werden sollen. Hexadezimal 32 bezeichnet ein Sparkonto, Hexadezimal 33 ein Kreditkartenkonto und Hexadezimal 34 ein Sonderkonto für die

Kontowahltaste, das um bis zu drei Dezimalstellen unmittelbar nach dem ersten TAS Byte modifiziert werden kann. Diese Zahlenmodifizierer haben im TAS Feld dieselbe Bedeutung wie im FAS Feld. Da das TAS Feld ebenfalls in der Länge veränderlich ist, muß auch ihm ein Feldtrennungsbyte (FS Byte) mit dem Dateninhalt hexadezimal FE folgen. Nach dem Feldtrennungsbyte für das Kontozugangswahlfeld werden die vom Magnetstreifen auf der Kreditkarte gelesenen Daten übertragen. Durch Entfernen des Päritätsbit aus dem vereinheitlichten Code der American Bankers Association kann man die beiden vier Bit großen Zeichen der Kreditkartendaten in jedes Nachrichtenbyte packen. Falls eine ungerade Zahl der Kreditkartenzeichen auf der Kreditkarte erscheint, wird das letzte Byte mit Hexadezimal F aufgefüllt, um alle Bytes der Nachricht zu füllen. Zeichen für den Anfang und das Ende der Kartenzeichen und die longitudinale Redundanzprüfung (LRC) werden insoweit aus der übertragenen Transaktionsanforderungsnachricht ausgeschlossen, als sie von der Station 14 geprüft werden.

Eine Zustandsnachricht von einer Station 14 an ein Datenverarbeitungssystem beginnt mit dem vier Byte großen gemeinsamen Vorlauffeld, welches die Nachrichtenlänge (L), die Transaktionszahl (N), die Nachrichtenklasse (C) und die Nachrichtenunterklasse (SC) für die Nachricht in den Bytepositionen 1 bis 4 angibt. Die Bytepositionen 5 bis 8 enthalten ein 32 Bit großes verschlüsseltes Feld, welches später genauer beschrieben wird, im allgemeinen jedoch eine Wiederholung der 8 Bit großen Transaktionszahl (N), acht die umlaufende Bargeldzahl für die Bestimmung 2 (CNTR2) darstellende Bits, acht die Anzahl der Zustandsbytes (CB) anzeigende Bits und acht die umlaufende Bargeldzahl für die Bestimmung 1 (CNTR1) darstellende Bits enthält. Das CB-Byte ist ein ein Byte großes Feld, welches eine binäre Zahl der Anzahl von Zustands- und Anfragedatenbytes enthält, die dem verschlüsselten Teil (Bytes 5-8) der Nachricht für eine normale Zustandsnachricht folgen. Für eine "Wiederholungsanforderungsnachricht" enthält das CB-Feld das "Aktionsfeld" von der Transaktionsantwort für die letzte Transaktionsanforderungsnachricht.

Das Aktionsfeld ist ein acht Bit großes Feld, welches als Teil des 32 Bit großen verschlüsselten Feldes einer Transaktionsantwortnachricht übertragen wird. Die acht Bit großen Zählerteile (CNTR) des 32 Bit großen verschlüsselten Feldes geben die binäre Zahl der Rechnungen an, die von der ersten und zweiten Bargeldausgabeeinrichtung ausgegeben wurden. Diese Zahlen werden von den Zählern abgenommen, die für jede ausgegebene Rechnung hochgeschaltet werden und von Hexadezimal FF nach Hexadezimal 00 überlaufen. Die Zahlen werden im Zusatzspeicher des Funktionsuntersystems 76 gespeichert, so daß die Zahl während eines kurzzeitigen Stromausfalles gerettet wird. Nach dem 32 Bit großen verschlüsselten Feld bei den Bytes 5-8 folgt ein Datenfeld, welches ein vier Byte großes Zustandsfeld in den Bytepositionen 9-12 enthält. Diese vier Bytes definieren den laufenden Zustand einer Transaktionsstation 14 gemäß späterer Beschreibung. Die meisten Zustandsnachrichten enden mit einem FS-Byte in der Byteposition 13. Eine Zustandsnachricht, die jedoch aufgrund einer Anfragebefehlsnachricht gesendet wird, enthält 112 der 128 Bytes, die im Zusatzspeicher des Untersystems 76 gespeichert sind, und nach den vier Zustandsbytes gesendet werden. Für diese Nachricht enthält das CB-Feld die Zahl 116. Die 16 Bytes des nicht flüchtigen Speichers, die nicht aufgrund einer Anfragenachricht gesendet werden, enthalten die beiden acht Byte großen Codierschlüssel. Wenn die Zustandsnachricht als Antwort auf eine Wiederholungsanforderungsnachricht gesendet wird, enthalten die vier Zustandsbytes die vier Bytes der letzten Transaktionszustandsnachricht, und diesen folgt die komplette ursprüngliche Transaktionsanforderungsnachricht. Diese Information gestattet dann dem Datenverarbeitungssystem die Zustände wieder herzustellen, die vor dem Vorfall herrschten, durch den das Datenverarbeitungssystem zur Anforderung der Wiederholung veranlaßt wurde.

Von den 32 Bitpositionen der vier Zustandsbytes auf den Bytepositionen 9-12 der Zustandsnachricht hat jede ihre vorbestimmte Bedeutung. Diese Bedeutungen sind der Definition des physikali-

schen und des Betriebszustandes einer Station 14 mit so hinreichender Eindeutigkeit zugeordnet, daß ein Datenverarbeitungssystem den allgemeinen Betrieb einer jeden Station 14 adressieren und steuern kann. Diese Bedeutungen sind nachfolgend in Tabellenform beschrieben, wobei die Zahl links die Zustandsbytezahl zwischen 0 und 3 darstellt, wobei das Zustandsbyte 0 in der Byteposition 9 der Zustandsnachricht steht und das Zustandsbyte 3 in der Byteposition 12. Jedem Zustandsbyte sind 8 Bits mit der Bezeichnung Bit 0 bis Bit 7 zugeordnet, wobei das Bit 0 in der werthöchsten Bitposition und das Bit 7 in der wertniedrigsten Bitposition steht.

Byte	Bit	Beschreibung
0	0	Zustandsbit für Transaktionsende. Diese Bitposition wird auf logisch 1 am Anfang einer jeden Transaktion gestellt, um anzuzeigen, daß die Transaktion noch nicht beendet ist, weil eine Transaktionsantwortnachricht gebraucht wird. Die Bitposition wird auf Logisch 0 zurückgesetzt, wenn eine Transaktion ausgeführt wurde gemäß Bestätigung in einer Transaktionsantwortnachricht.
0	1	Ungültige Transaktionsreihenfolgezahl im Transaktionsantwortbit. Diese Bitposition wird jedesmal bei Beginn einer neuen Transaktion auf Logisch 0 zurückgestellt. Die Bitposition wird jedesmal auf Logisch 1 gesetzt, wenn die Transaktionszahl (N) innerhalb des gemeinsamen Vorlauffeldes einer vom Datenverarbeitungssystem empfangenen Nachricht ungenau ist. Eine Ausnahme wird für eine Echonachricht gemacht, die keine bedeutungsvolle Information in die Transaktionszahlenposition des Vorlauffeldes überträgt.
0	2	Ungültige Transaktionsunterklasse im Antwortnachrichtenbit. Diese Bitposition wird jedesmal auf Logisch 0 zurückgestellt, wenn eine neue Transaktion begonnen wird, und sie wird jedesmal auf Logisch 1 gesetzt, wenn eine Transaktionsantwortnachricht empfangen wird, die in dem vierten oder Unterklassenbyte des gemeinsamen Vorlauffeldes von dieser Transaktionsanforderungsnachricht eine andere Zahl enthält. Byte 0, Bit 0 müssen gleichzeitig mit dieser Bitposition gesetzt werden.

0	2	Ungültige Transaktionsunterklasse im Antwortnachrichtenbit. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt und jedesmal auf Logisch 1 gestellt, wenn das Unterklassenbyte einer Transaktionsantwortnachricht nicht mit dem Unterklassenbyte der entsprechenden Transaktionsanforderungsnachricht übereinstimmt. Byte 0, Bit 0 müssen jedesmal gesetzt werden, wenn diese Bitposition gesetzt wird.
0	3	Ungültiges Klassenbit. Diese Bitposition wird auf 0 zurückgestellt, nachdem eine Ausnahmezustandsnachricht gesendet wurde und es wird jedesmal auf Logisch 1 gesetzt, wenn eine Nachricht vom Datenverarbeitungssystem empfangen wird, die eine ungültige Klassenbezeichnung im Byte 3 des gemeinsamen Vorlauffeldes enthält. So kann beispielsweise eine Transaktionsstation 14 eine nicht angeforderte Initialisierungsnachricht (IPL) oder eine nicht angeforderte Transaktionsantwortnachricht empfangen.
0	4	Betragsfehler im Transaktionsantwortnachrichtenbit. Diese Bitposition wird am Anfang einer jeden neuen Transaktion auf Logisch 0 zurückgestellt und jedesmal auf Logisch 1 gestellt, wenn eine Transaktionsantwortnachricht empfangen wird, in der das Dollarbetragsbyte im verschlüsselten Feld einen falschen Dollarbetrag anzeigt. Das Bit 0, das Byte 0 (AMT) muß jedesmal auf Logisch 1 gesetzt werden, wenn diese Bitposition auf Logisch 1 gesetzt wird.

0	5	Nicht zugeordnet.
0	6	Vom Kunden gestrichenes Transaktionsbit. Diese Bitposition wird am Anfang einer jeden neuen Übertragung auf Logisch 0 zurückgestellt und in dem Fall auf Logisch 1 gestellt, in dem ein Kunde eine auf der Benutzertastatur gelöschte Taste nach der Übertragung der Transaktion einer Transaktionsanforderungsnachricht betätigt.
0	7	Benutzerzeitsperrebit. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf 0 zurückgestellt und jedesmal auf Logisch 1 gesetzt, wenn ein Benutzer mehr als eine vorgegebene Zeit für die Eingabe einer Zahl über die Benutzertastatur oder für das Ablegen von Material durch die Depositenklappe braucht. Bit 0 des Byte 0 müssen jedesmal gesetzt werden, wenn diese Position oder die Position 06 auf Logisch 1 gesetzt werden.
1	0	Befehlsrückweisungsbit. Diese Bitposition wird nach dem Senden einer Befehlszustandsnachricht auf Logisch 0 zurückgestellt. Die Bitposition wird bei Empfang einer Befehlsnachricht auf Logisch 1 gestellt, die nicht ausgeführt werden kann, weil die Transaktionsstation 14 zu der Zeit des Befehlsempfanges belegt ist.
1	1	Ungültiges Befehlsbit. Diese Bitposition wird beim Senden einer Befehlszustandsnachricht auf Logisch 0 zurückgestellt. Die Bitposition wird jedesmal auf Logisch 1 gesetzt,

wenn eine Befehlsnachricht mit fehlenden Feldern darin empfangen wird. Ein Schlüsseländerungsbefehl beispielsweise, der den neuen Schlüssel nicht enthält oder ein Bildanzeigeänderungsbefehl, ohne ein neues Bildanzeigefeld, können diese Bitposition auf Logisch 1 setzen. Diese Bitposition wird auch auf Logisch 1 gesetzt durch eine Befehlsnachricht, die im Byte 4 des gemeinsamen Vorlauffeldes eine ungültige Unterklassenbezeichnung enthält.

1 2 IPL Anforderungsbit. Diese Bitposition wird beim richtigen Empfang einer Ladeinitialisierungsnachricht vom Datenverarbeitungssystem auf Logisch 0 zurückgestellt und jedesmal auf Logisch 1 gesetzt, wenn eine Transaktionsstation 14 von dem geschlossenen in einen offenen Zustand übergeht, beispielsweise beim Schließen der Bediener-Wartungstechniker-Zugangsklappe oder auf Befehl vom Datenverarbeitungssystem. Dieses Bit wird ebenfalls jedesmal auf Logisch 1 gesetzt, wenn eine Datenstation eine Befehlsnachricht empfängt, die der Station die Anforderung eines IPL befiehlt.

1 3 IPL und Prozessbit. Diese Bitposition dient als Modizfizierbit für die Bitposition 2 des Byte 1. Eine Kombination des Bit 2 und des Bit 3 gleich 00 zeigt an, daß die Station initialisiert ist. Dieser Zustand kann nur auftreten, wenn sich die Station in einem offenen Zustand befindet. Die Kombination der Bitposition 2 und 3 gleich 10 zeigt an, daß die Initialisierung angefordert, die Ladeinitialisierungsnachricht jedoch noch nicht empfan-

gen wurde. Ein Kombination der Bitposition 2, 3 gleich 11 zeigt an, daß eine Ladeinitialisierung ungerade läuft.

1 4 Bargeldzähler-Fehlerbit. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt. Die Bitposition wird jedesmal auf Logisch 1 gesetzt, wenn eine Transaktionsantwortnachricht empfangen wird, die ein Bargeldzählerbyte (CNTR) innerhalb des verschlüsselten Feldes enthält, welches nicht mit dem Zustand des Bargeldzählers in der Station übereinstimmt. Der Bargeldzähler ist ein Überlaufzähler, der jedesmal mit Ausgabe einer neuen Rechnung hochgeschaltet wird. Byte 0, Bit 0 muß jedesmal auf Logisch 1 gesetzt werden, wenn diese Bitposition auf Logisch 1 gesetzt wird.

1 5 C- und CS-Feld-Fehlerbit. Diese Bitposition wird beim Senden einer Ausnahmezustandsnachricht auf Logisch 0 zurückgestellt. Diese Bitposition wird auf Logisch 1 gestellt bei Empfang einer Befehlsnachricht vom Datenverarbeitungssystem, die ein Klassen- und Unterklassenbyte (C und SC) im verschlüsselten Datenfeld enthält, die nicht mit dem Klassen- und Unterklassenbyte des gemeinsamen Vorlauffeldes übereinstimmen. Dieser Übereinstimmungsfehler zeigt einen möglichen Fehler bei der Codierschlüsselsynchronisation oder einen Fehler in der Datenverarbeitungsanlage an. In einer normalen Befehlsnachricht sind die beiden Bytes für Klasse und Unterklasse (C und SC) des gemeinsamen Vorlauffeldes zu einem Klassen- und Unterklassenbyte kombiniert

(gepackt durch Abfühlen der vier führenden Nullbits eines jeden Byte).

1	6	Kommunikations- oder Transaktionszeitsperre, Antwortreihenfolgebit. Am Anfang einer jeden neuen Benutzertransaktion wird diese Bitposition auf Logisch 0 zurückgestellt. Die Bitposition wird jedesmal auf Logich 1 gestellt, wenn eine vorgegebene Zeit nach Übertragung einer Benutzertransaktionsanforderungsnachricht abgelaufen ist, ohne daß eine entsprechende Transaktionsantwortnachricht empfangen wird. Wenn diese Bitposition auf Logisch 1 gesetzt wird, muß jedesmal auch Byte 0, Bit 0 auf Logisch 1 gesetzt werden.
1	7	Nicht erkennbares Nachrichtenbit. Diese Bitposition wird nach dem Senden einer Ausnahmezustandsnachricht auf Logisch 0 zurückgestellt. Sie wird jedesmal auf Logisch 1 gesetzt zur Bezeichnung einer nichterkennbaren Nachricht, wenn eine Nachricht empfangen wird, die dem verlangten vorgegebenen Nachrichtenformat nicht entspricht. Die Anzahl von Bytes kann beispielsweise nicht mit der Bezeichnung der Nachrichtenlänge (L) im gemeinsamen Vorlauffeld übereinstimmen oder es kann beim Lesen eines Datenbyte ein Paritätsfehler auftreten oder eine Byteposition kann ungültige Daten enthalten.
2	0	Kartenrückhaltebit. Dieses Bit wird auf Logisch 0 am Anfang einer jeden neuen Benutzertransaktion zurückgestellt und auf Logisch 1 jedesmal gestellt, wenn eine vom Benutzer

angeforderte Transaktion beendet ist und die Transaktionsstation 14 die vom Benutzer eingelegte Kreditkarte einbehält. Diese Bitposition zeigt an, daß die Karte aufgrund eines Maschinenfehlers an der Transaktionsstation 14 einbehalten wurde und nicht aufgrund eines Befehles von der Datenverarbeitungsanlage.

2 1 Ausgabefehlerbit. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt. Die Bitposition wird jedesmal auf Logisch 1 gestellt, wenn während der Ausgabe eines Beleges wie beispielsweise einer Rechnung oder einer Transaktionsbestätigung ein Fehler auftritt. Diese Bitposition wird jedesmal gesetzt, wenn ein Beleg von einem Übertragungsbereich in einen Rückhaltebehälter abgelegt wird. Da die Transaktion bei der Wiederholung fertig sein kann, zeigt diese Bitposition nicht unbedingt eine unvollständige Benutzertransaktion an.

2 2 Fehlerbit für nicht erholungsfähige Ablage. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt. Sie wird auf Logisch 1 jedesmal dann gestellt, wenn eine Fehlerbedingung wie beispielsweise eine Verklemmung in der Ablage der Station auftritt und die Station aus dieser Fehlerbedingung nicht mehr herausfinden kann.

2	3	Überlaufbit der Anzeigetabelle. Diese Bitposition wird beim Senden einer Zustandsnachricht auf Logisch 0 zurückgestellt. Die Bitposition wird bei Empfang einer Befehlsnachricht zum Ändern der Bildanzeige von der Datenverarbeitungsanlage auf Logisch 1 gestellt, wenn diese Nachricht mehr Anzeigedaten enthält, als das Bildanzeigesystem der Station verarbeiten kann. Eine falsche Bildanzeigenachricht wird von der Station 14 nicht akzeptiert.
2	4	Nicht zugeordnet.
2	5	Nicht zugeordnet.
2	6	Nicht zugeordnet. Bit für erforderliches Eingreifen. Dieses Bit wird gesetzt, wenn eine Situation auftritt, in der ein Eingreifen erforderlich ist. Es wird zurückgestellt, wenn der Anzeiger für ein erforderliches Eingreifen abgeschaltet wird.
2	7	Zeitsperrbit für Kartenentnahme. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt. Die Bitposition wird auf Logisch 1 gesetzt, sobald eine vorgegebene Periode abläuft, nachdem die Kreditkarte einem Benutzer zur Verfügung gestellt wurde, ohne daß die Kreditkarte aus der Station 14 entnommen wurde. Diese Bitposition zeigt an, daß irgendein Eingreifen erforderlich ist. Normalerweise antwortet das Datenverarbeitungssystem durch einen Befehl an die Station, die Kreditkarte zurückzuhalten.

3	0	Offen/geschlossen-Bit. Diese Bitposition wird jedesmal auf Logisch 0 zurückgestellt, wenn die Station öffnet und zum Empfang einer Benutzertransaktionsanforderung bereit ist. Die Bitposition wird jedesmal auf Logisch 1 gestellt, wenn die Station schließt.
3	1	Bargeldausgabe-Bedingungsbit. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion zurückgestellt. Die Bitposition spricht auf einen Maschinenschalter an, der anzeigt, ob genug Bargeld in der Station gespeichert ist oder nicht, um eine maximale Bargeldausgabe durchzuführen. Die Bitposition wird jedesmal auf Logisch 1 gestellt, wenn bei der Ausführung einer vorhergehenden Bargeldausgabe, welcher die Zustandsnachricht entspricht, der Bargeldausgangszustand auftritt. Das Einschalten dieser Bitposition zeigt an, daß ein Eingreifen erforderlich ist und veranlaßt das Schließen der Station.
3	2	Bit für ungültigen Codierschlüssel. Diese Bitposition wird beim Senden einer Zustandsnachricht auf Logisch 0 zurückgestellt und auf Logisch 1 gestellt beim Empfang einer Befehlsnachricht zum Ändern des Schlüssels vom Datenverarbeitungssystem, die einen falschen Codierschlüsssel enthält (ein falscher Codierschlüssel enthält lauter Nullen).
3	3	Formularauslaufbit für Transaktionsbeleggeber. Diese Bitposition wird am Anfang einer jeden neuen Benutzertransaktion auf Logisch 0 zurückgestellt. Sie wird auf Logisch 1 gestellt,

wenn ein Transaktionsbelegfühler anzeigt, daß das letzte nutzbare Transaktionsbelegformular während der letzten vorhergehenden Transaktion ausgegeben wird, der die Zustandsnachricht entspricht.

3 4 Bit für geöffnete Ablagenklappe (Tür) oder Ausgabetor. Diese Bitposition wird beim Senden einer Zustandsnachricht zurückgestellt. Die Bitposition wird auf Logisch 1 gesetzt, wenn die Ablageklappe oder das Ausgabetor geöffnet bleiben, wenn sie geschlossen sein sollten, und zeigt an, daß die Klappe oder das Tor mit Gewalt geöffnet wurden.

3 5 Bit für nicht behebbaren Maschinenfehler. Diese Bitposition wird nach dem Einschalten einer Ausnahmezustandsnachricht auf Logisch 0 gesetzt. Die Bitposition wird jedesmal auf Logisch 1 gesetzt, wenn eine Verklemmung oder eine andere Fehlerbedingung auftritt, die nicht behoben werden kann, sei es während der Ausführung einer Transaktion oder zu irgendeiner anderen Zeit. Das Einschalten dieser Bitposition zeigt an, daß ein Eingreifen erforderlich ist und die Station schließt.

3 5 Bit für geöffnete Kundentür. Diese Bitposition wird beim Senden einer Zustandsnachricht auf Logisch 0 zurückgestellt. Die Bitposition wird auf Logisch 1 gestellt, wenn die Kundentür, die Zugang zur Benutzertastatur und zur Bildanzeige gibt, offen ist, wenn sie geschlossen sein sollte und die Position zeigt an, daß die Tür mit Gewalt geöffnet wurde.

Wenn dieses Bit eingeschaltet ist, ist ein Eingreifen erforderlich und die Station schließt.

3	7	Sicherheitsschloß-Verriegelungsbit. Diese Bitposition wird auf Logisch 0 zurückgestellt, wenn die Bedienerzugangstür geschlossen ist und wird auf Logisch 1 gestellt, wenn die Tür offen ist. Jedesmal wenn diese Bitposition auf Logisch 1 gestellt wird, schließt die Station 14.

Eine Transaktionsantwortnachricht von einem Datenverarbeitungssystem 12 an eine Benutzerstation 14 wird als Antwort auf eine Benutzertransaktionsantwortnachricht erzeugt. Die Transaktionsantwortnachricht beginnt mit dem einheitlichen vier Byte großen gemeinsamen Vorlauffeld, welches die Gesamtnachrichtenlänge (L), die Transaktionszahl (N), die Nachrichtenklasse (C) und die Nachrichtenunterklasse (SC) angibt. Es folgen 4 Bytes oder 32 Bits verschlüsselter Information, ein Bilddatenfeld mit veränderlicher Länge, ein Feldtrennzeichen (FS) und ein Transaktionsbelegdruckfeld mit wahlfrei veränderlicher Länge sowie ein letztes Feldtrennzeichen (FS). Das 4 Byte große verschlüsselte Feld enthält eine 1 Byte große Bargeldzählerzahl Nr. 2 (CNTR2), ein Aktionsbyte, eine 1 Byte große Bargeldzählerzahl Nr. 1 (CNTR1) und ein Betragsbyte (AMT), welches die Anzahl von Rechnungen angibt, für die die Antwortnachricht die Ausgabe genehmigt. Die Station 14 prüft diesen genehmigten Betrag durch Vergleich mit der Anforderung.

Das Aktionsbyte ist eine ein Byte große Anweisung vomm Datenverarbeitungssystem 12, die die Station 14 anweist, eine Benutzertransaktion entsprechend deren Dateninhalt zu verarbeiten.

Bit 0. Wenn Bit 0 auf Logisch 1 gesetzt ist, erhält die Station 14 den Befehl, sofort eine Standard-Bildanzeigenachricht anzuzeigen, die bezeichnet ist durch das wahlfreie Bilddatenfeld, welches unmittelbar dem codierten Feld folgt. Bis zu 128 separaten Nachrichten mit den Bezeichnungen 0-127, sind in dem zum Mikroprozessor 60 gehörenden Datenspeicher 66 gespeichert. Wenn Bit 0 des Aktionsbyte auf Logisch 1 gesetzt ist, erhält die Station 14 den Befehl, eine dieser Nachrichten anzuzeigen, die durch den binären Inhalt des 1 Byte großen wahlfreien Bildfeldes an der Byteposition 9 der Transaktionsantwortnachricht bezeichnet ist.

Bit 1. Wenn Bit 1 auf Logisch 1 steht, erhält die Station 14 den Befehl, sofort eine wahlfreie Bildanzeigenachricht anzuzeigen, die im wahlfreien Bilddatenfeld unmittelbar hinter dem codierten Feld enthalten ist. Wenn Bit 1 auf Logisch 1 gesetzt wird, enthält Byte 9 am Anfang des wahlfreien Bilddatenfeldes eine binäre Zahl, die die Länge der Bildnachricht in Bytes ausschließlich Byte 9 angibt. Unmittelbar hinter Byte 9 enthält die Transaktionsantwortnachricht den Text der gewünschten Bildnachricht im EBCDIC Code, wobei jedes Byte ein Bildzeichen angibt.

Bit 2. Eine logische Eins an der Bitposition 2 des Aktionsbyte gibt an, daß eine Transaktionsstation 14 den Befehl erhält, Information auf einen Transaktionsbeleg zu drucken und diese logische Eins besagt weiterhin, daß das Trennungsaktionsbeleg-Druckdatenfeld der Antwortnachricht die Daten enthält, die im EBCDIC Code zu drucken sind.

Bit 3 nicht definiert.

Bit 4. Eine logische Eins in der Bitposition 4 besagt, daß eine angeforderte Benutzertransaktion wie angefordert genehmigt ist.

Bit 5. Eine logische Eins in dieser Bitposition sagt, daß die Kreditkarte eines Benutzers durch die Station 14 einzubehalten

ist, während eine logische Null anzeigt, daß die Kreditkarte an den Benutzer zurückzugeben ist.

Bit 6. Eine logische 1 in dieser Bitposition gibt an, daß der Benutzer die Transaktion bestätigen muß, bevor die Station 14 mit der Ausführung fortfährt. Der Benutzer bestätigt die Transaktion durch Betätigen entweder eine Löschtaste oder einer Fortführtaste in einem Tastatursteuerfeld. Typischerweise erfolgt eine Anzeige der Transaktion zu dem Zeitpunkt, an dem der Benutzer eine Taste wählt. Die Nachricht "50 DOLLAR VON SPARKONTO AUF SCHECKKONTO ÜBERTRAGEN - Taste löschen oder Fortfahren drücken" kann z. B. angezeigt werden.

Bit 7 nicht definiert.

Das Transaktionsbeleg-Druckfeld am Ende einer Transaktionsantwortnachricht ist in mehrere Unterfelder geteilt, die die Kommunikation von Druckdaten für bis zu zwei Transaktionsbelegformulare gestatten. Das erste Unterfeld ist ein gemeinsames Datenunterfeld, welches Information enthält wie beipielsweise den Namen und die Kontonummer des Benutzers, die für beide Transaktionsbelege dieselben sind. Ein gemeinsames Datenfeld kann entweder eine Station 14 mit dem Druck einer im Speicher 66 einer Station 14 gespeicherten Drucknachricht beauftragen oder die Station anweisen, eine Nachricht zu drucken, die als Teil eines gemeinsamen Datenfeldes und des Standard EBCDIC Code gesendet wird. Das erste Byte eines gemeinsamen Datenfeldes bestimmt die Quelle der Druckdaten. Wenn dieses Byte eine Zahl von 1 bis 127 (Unterhexadezimal 80) enthält, sind die Druckdaten in Standard EBCDIC Form im gemeinsamen Datenunterfeld unmittelbar hinter dem ersten Byte enthalten. In diesem Fall stellt das erste Byte eine binäre Längenzahl dar, die die Anzahl von Textbytes im gemeinsamen Datenfeld ausschließlich des Längenbyte angibt. Wenn die gemeinsamen Druckdaten durch eine gespeicherte Nachricht geliefert werden sollen, wird zu den 128 (Hexadezimal 80) eine Drucknachrichtenidentifizierungsnummer, die

die jeweilige gespeicherte Nachricht bezeichnet, als erstes und einziges Byte des gemeinsamen Datenunterfeldes gesendet. Wenn die gemeinsamen Daten beispielsweise der gespeicherten Nachricht Nr. 30 entnommen werden sollen, dann würde das ein Byte große gemeinsame Datenfeld die binäre Zahl 30 + 128 = 158 (Hexadezimal 9E) enthalten. Mit dem ein Byte großen Dateninhalt entsprechende Identifizierungszahl 0 (Hexadezimal 80) werden die gemeinsamen Daten und die Belegdaten abgegrenzt und dieses Byte darf nicht zur Definition der Nachricht Ø als gespeicherte Nachricht benutzt werden. Ein Datenunterfeld mit der Anweisung Nr. 1 folgt unmittelbar einem Begrenzerbyte Hexadezimal 80 hinter dem gemeinsamen Datenunterfeld. Das Datenunterfeld mit der Anweisung Nr. 1 kann eine echte EBCDIC-Drucknachricht enthalten oder eine gespeicherte Drucknachricht bezeichnen und benutzt dasselbe Format, wie das gemeinsame Datenunterfeld. Durch das Datenunterfeld für die Anweisung Nr. 1 befohlene Druckinformation wird jedoch nur auf ein mit Formular Nr. 1 bezeichnetes Transaktionsbelegformular gedruckt. Das Begrenzungszeichen (Hexadezimal 80) folgt unmittelbaar dem Datenunterfeld für die Anweisung Nr. 1. Dem zweiten Begrenzungszeichen folgt direkt das Datenunterfeld für die Anweisung Nr. 2. Das Bestätigungsdatenunterfeld Nr. 2 hat ein ähnliches Format und ähnlichen Dateninhalt wie das gemeinsame Datenunterfeld und das Belegdatenunterfeld Nr. 1. Das Datenunterfeld Nr. 2 kann entweder eine gesendete Drucknachricht im EBCDIC Code enthalten oder eine gespeicherte Drucknachricht bezeichnen. Wenn das Belegdatenunterfeld Nr. 2 nicht vorhanden ist, d. h. eine Länge von 0 Bytes hat, wird ein zweites Transaktionsbelegformular weder gedruckt noch ausgegeben. Ein Feldtrennzeichen (FS) folgt diesem Belegdatenunterfeld Nr. 2 unmittelbar und bezeichnet das Ende des Transaktionsbelegdruckfeldes und das Ende einer Transaktionsantwortnachricht. Ein Transaktionsbelegformular wird links oben in der Ecke beginnend und dann zeilenweise von links nach rechts im allgemeinen Leseformat bedruckt. Ein EBCDIC Wagensteuercode wird benutzt, um eine Textzeile zu beenden und das Drucken des nächsten Textzeichens in der äußersten linken Zeichenposition der

nächsten Zeile zu beginnen. Die Druckoperation verfolgt eine vorgegebene Reihenfolge, in der gemeinsamer Text zuerst auf dem Belegformular 1 gedruckt wird, dann wird der Belegtext 1 auf dem Belegformular 1 gedruckt, dann der allgemeine Text auf dem Belegformular 2 und schließlich der Belegtext auf dem Belegformulur 2.

Vom Datenverarbeitungssytem 12 wird an eine Transaktionsstation 14 eine Befehlsnachricht gesendet, um den Betrieb oder den Zustand der Station nach dem Dateninhalt der Befehlsnachricht zu steuern. Jede Befehlsnachricht beginnt mit einem vier Byte großen gemeinsamen Vorlauffeld, daß die Nachrichtenlänge (L), die Transaktionszahl (N), die Nachrichtenklasse (C) und die Nachrichtenunterklasse (SC) enthält. Dann folgt ein vier Byte großes verschlüsseltes Feld, welches das Bargeldzählerbyte (CNTR1), das Klassen- und Unterklassenbyte, welches die zu einem Byte kombinierte Klassen- und Unterklassenbezeichnung enthält, ein zweites Bargeldzählerbyte (CNTR2) und ein Spezialbyte (SPEC). Das Spezialbyte wird für eine Anfragebefehlsnachricht benutzt, um die Information anzuzeigen, die von einer angesprochenen Station durch eine Antwortzustandsnachricht an das Datenverarbeitungssystem zu geben ist. Die Bits 0 bis 4 des Spezialbyte sind nicht zugeordnet und werden normalerweise als Logisch 0 übertragen. Bit 5 wird auf Logisch 1 gesetzt, um anzuzeigen, daß eine Station angesprochen wurde oder ihre letzte Zustandsnachricht zurücksendet. Bit 6 wird auf Logisch 1 gesetzt um anzuzeigen, daß die Station eine laufende Zustandsnachricht und die 112 Bytes des Zusatzspeichers im Funktionsuntersystem 76 übertragen muß, die die beiden Codierschlüssel nicht enthalten. Eine logische Eins im Bit 7 des Spezialbytes zeigt an, daß die Station den Befehl erhalten hat, eine normale Zustandsnachricht zu senden. Die Bits 5, 6 und 7 sind gegenseitig exklusiv, wobei nur jeweils eines eingeschaltet sein sollte.

Im gemeinsamen Vorlauffeld und einem vier Byte großen codierten Feld einer Befehlsnachricht folgen zwei wahlfrei zu verschlüsselnde Felder. Das erste dieser Felder führt die erste Hälfte eines acht Byte großen Codeschlüssels und das zweite die zweite Hälfte. Dieses erste unß zweite wahlfrei verschlüsselbare folgen nur nach einem Schlüsselschaltbefehl oder einem Schlüsseländerungsbefehl. Eine Station 14 reagiert auf einen Schlüsseländerungsbefehl durch Entschlüsselung der Befehlsnachricht mit dem alten dritten oder Übertragungscodeschlüssel (Schlüssel B) und ersetzt dann den in den beiden wahlfrei codierbaren Feldern 1 und 2 für alle künftigen Kommunikationen ein. Ein Schlüsseleinschaltbefehl wirkt genauso wie ein Schlüsseländerungsbefehl, jedoch wird der neue Schlüssel zu einem Rückgriffschlüssel (C) codiert, der im Hilfsspeicher gespeichert wird. Bei einer Befehlsnachricht "Bildanzeigenachricht ändern" sind die beiden wahlfrei codierbaren Felder in der Nachricht nicht eingeschlossen sondern dem vier Byte großen codierten Feld folgt ein Datenfeld mit wahlfreiem Klartext. Dieses Datenfeld beginnt mit einer Indexzahl (IDX), der ein Datenfeld-Längenbyte (LD) und der neue Bildanzeigetext im Standard EBCDIC Code folgt. Eine solche Befehlsnachricht beeinflußt die eigentliche für den Stationsbenutzer sichtbare Bildanzeige nicht sondern verändert stattdessen den Dateninhalt einer im Datenspeicher 66 gespeicherten Bildanzeigenachricht. Wenn z. B. die gespeicherte Bildanzeigenachricht "Kreditkarte herausnehmen" ersetzt werden soll durch eine Bildanzeigenachricht der Identifizierungsnummer 40 auf "Kreditkarte entfernen", dann enthält das Indexbyte (INDX) die Bildanzeigenachrichtidentifizierungsnummer der gespeicherten Nachricht, die geändert werden soll. Das Datenfeldlängenbyte (LD) enthält eine binäre Zahl, die die Anzahl von Bytes im Text der neuen Nachricht angibt, die unmittelbar folgt. Wenn die neue Nachricht zu lang ist, um in die in der Tabelle der Bildanzeigenachrichten im Datenspeicher 66 verfügbare Anzahl von Bytes zu passen, wird der Befehl nicht ausgeführt und die folgende Zustandsnachricht zeigt das an. Weil die Bildanzeigenachrichten veränderliche Länge haben und alle Nachrichten vom

Datenverarbeitungssystem an eine Station 14 eine gerade Anzahl von Bytes enthalten müssen, muß eventuell das Ende des Bildanzeigetextes mit einem willkürlichen Füllzeichen aufgefüllt werden. Dieses Füllzeichen wird nicht im Datenfeldlängenbyte (LD) mitgezählt, sondern im Gesamtnachrichtenlängenbyte (L) im gemeinsamen Vorlauffeld der Befehlsnachricht.

Die Ladeinitialisierungsnachricht liefert die Information für den Randomspeicherteil des Datenspeichers 66, die im Falle eines Stromausfalles verlorengehen kann. Sie kann auch Reinitialisierung der Station verwendet werden. Die Nachricht beginnt mit dem einheitlichen vier Byte großen gemeinsamen Vorlauffeld, dem ein zwei Byte großes binäres Zahlenfeld folgt, welches die Anzahl von Bytes in dem nachfolgenden Datenfeld angibt. Das Datenfeld enthält das letzte Feld der Ladeinitialisierungsnachricht und das im Datenspeicher 66 gespeicherte Bild. Die kritische Information wie Mikroprogrammroutinen und Einrichtungswahlbytes im Datenfeld wird mit dem dritten Übertragunsschlüssel (B) in vier sequentiellen Bytesegmenten verschlüsselt.

Im allgemeinen liefert das während der Initialisierung empfangene Benutzungsbild, die Information, die sich von einer Station zu andern ändern kann und ist daher nicht einfach durch Festwertspeicher implementiert. In dem Bild sind die gespeicherte Benutzeranzeige und Drucknachrichten enthalten, die bis zu 49 vorgegebene Nachrichten mit der Bezeichnung 1 bis 49 einschließen können. Als Nachricht 50 ist auch eine Fonttabelle eingeschlossen, die bis zu 574 Bytes umfaßt, mit denen Nicht-Standardzeichen oder Graphiken dargestellt werden können, die durch einen gegebenen Stationskunden wie beispielsweise eine Bank gewählt wurden. Außerdem sind in dem Bild in bestimmten Ausmaß Programmier- und Programmsteuerinformationen für die spezielle Kombination verfügbarer Zusätze vorhanden, die in einer gegebenen Station implementiert sind.

AUFBAU DER TRANSAKTIONSNACHRICHT

Die Kommunikation zwischen einem Datenverarbeitungssystem 12 und einer Transaktionsstation 14 während der Ausführung einer vom Benutzer angeforderten Transaktion werden im einzelnen anhand des Blockdiagrammes in den Fig. 3 bis 5 beschrieben. Das Kommunikationssystem und seine Arbeitsweie werden anhand spezifischer Beispiele beschrieben, die jedoch keinerlei Einschränkung für die Möglichkeiten der Station 14 darstellen.

Als spezifisches Beispiel wird angenommen, daß die Station 14 in der Wand einer Bankzweigstelle eingebaut ist. Die Station ist ähnlich wie die Station 46 in Fig. 1 in einer geschlossenen Schleife an ein Steuergerät 32 und über dieses an ein Datenverarbeitungssystem 12 angeschlossen. Die Kommunikationseinrichtungen für den Benutzer der Station 46, die in einer Außenwand der Bank eingebaut ist, befinden sich außerhalb des Gebäudes und der größte Teil der Station innerhalb der Bank. Die Bedienertafel ist über die Wartungsklappe vom inneren der Bankzweigstelle her zugänglich. Wenn sich ein potentieller Kunde der Station 46 nähert, zeigen die Beleuchtung des Tastaturbereiches und ein Zeichen an der Vorderseite der Station an, daß die Station Betriebsbereit ist (offen). Ist die Beleuchtung nicht eingeschaltet und leuchtet eine Anzeige "geschlossen" auf, heißt das, daß die Station für die Ausführung von Transaktionen nicht zur Verfügung steht und jede Handlung des Benutzers ignoriert wird. Wenn die Station geöffnet ist, leitet der Benutzer eine Transaktion dadurch ein, daß er seine Kreditkarte in einen Schlitz steckt. Im vorliegenden Beispiel sei angenommen, daß ein Benutzer Geld von seinem Sparkonto auf sein Scheckkonto übertragen will.

1. TRANSAKTIONSANFORDERUNGSNACHRICHT

Der erste Teil der dreiteiligen Kommunikationsfolge bei einer Benutzertransaktion ist in Fig. 3 gezeigt. Der Mikroprozessor 60 in der Station ist allgemein dargestellt, spezifische Verbindungen

zu physikalischen oder Funktionsblocks sind nicht gezeigt. Die logische Verbindung erfolgt gemäß der Darstellung in Fig. 2 und die Betriebssteuerung und Datenverarbeitung werden vom Mikroprozessor 60 vorgenommen.

Wenn der künftige Benutzer von seiner Bank eine Kreditkarte 100 ausgehändigt bekommt, wird ihm auch eine sechsstellige persönliche Kenummer (ID) zugeteilt. Diese persönliche kann wahlfrei zu der auf einem Streifen magnetischen Materials auf der Kreditkarte 100 aufgezeichneten Information in Beziehung gesetzt werden. Wenn die Kreditkarte in die Station 46 eingelegt wird, wird das Vorhandensein der Karte abgefühlt und ein Kreditkartentransportmechanismus zieht die Karte in die Station 14 und an einem Lesekopf vorbei, wo sie auf richtige Ausrichtung und einwandfreien Zustand abgefühlt wird. Wenn die Karte falsch ausgerichtet ist, unlesbare Daten enthält oder von einem Typ ist, der von der Station 46 nicht angenommen werden kann, wird sie zurückgegeben. (Wenn die Karte abgelaufen ist, kann sie auf Befehl des Datenverarbeitungssystems einbehalten werden). Nimmt man an, daß die Kreditkarte 100 in Ordnung ist, so wird sie an einem Kartenleser 102 vorbeitransportiert, wo die Information auf dem Magnetstreifen gelesen und im Randomspeicherteil des Datenspeichers 66 gespeichert wird. Dann wird die Karte in einem Kartenübertragungshaltebereich festgehalten. Die Kreditkarte 100 muß mit den durch die American Bankers Association festgelegten Normen verträglich sein. Das heißt, daß der Magnetstreifen eine Folge von fünf Bitwörtern enthält, die ein Paritätsbit und vier Datenbits darstellen. Die vier Datenbits enthalten ein Kartenanfangszeichen (SOC), ein Feldtrennzeichen und ein Kartenendzeichen (EOC). Zahlen sind in binär codierter Dezimalform dargestellt. Ein typisches Magnetstreifenformat beginnt mit einem Kartenanfangszeichen (SOC), dem eine Kontonummer von bis zu 19 Zeichen, dann ein Feldtrennzeichen, vier Zeichen, die das Ablaufdatum der Karte mit Monat und Jahr angeben, ein Diskretionsdatenfeld, ein Kartenendzeichen (EOC) und ein Zeichen für die longitudinale Redundanzprüfung

folgen. Auf dem Magnetstreifen können maximal 40 je fünf Bit große Zeichen aufgezeichnet werden. Wenn die Zeichen gelesen werden, bestimmt ein als Initialisierungszusatz vorgesehener Auswahlschlüssel k1 einen Anfangspunkt zum Auswählen acht aufeinanderfolgende Zeichen aus dem Magnetstreifen. Wenn k1 z. B. die Zahl 5 enthält, dann werden im Schritt 104 das fünfte bis dreizehnte Zeichen nach dem SOM ohne Paritätsbits zur Bildung von 32 Bits ausgewählt. Diese 32 Bits werden in einem Verschlüsselungsalgorithmus 106 verarbeitet und 32 Bits verschlüsselter Daten erzeugt.

Der Vergleich eines Teiles oder der ganzen persönlichen Kennnummer mit entsprechender Kreditkarteninformation, kann wahlweise auf Wunsch des Kunden vorgesehen werden, und diese wird dann zur Zeit der Initialisierung angegeben. Wenn der Vergleichszusatz nicht gewählt wird, kann die Korrespondenz zwischen persönlicher Kennummer und Kreditkarteninformation willkürlich gewählt werden. Die Ausführung eines Korrespondenzvergleiches ist jedoch dann unmöglich, wenn die Station 14 unter Steuerung eines unabhängigen Datenverarbeitungssystems läuft. Wenn die lokale Prüfzusatzeinrichtung gewählt wird, geben zwei Schlüssel an, wie die Prüfung auszuführen ist.

Der erste Schlüssel k1 gestattet die Auswahl einer zusammenhängenden Gruppe von 8 von der Kreditkarte gelesenen Zeichen. Der Schlüssel k1 gibt die Position des ersten dieser 8 Zeichen hinter dem SOM an. Die 8 Zeichen wählt man typischerweise, aber nicht notwendigerweise so, daß die ganz innerhalb des Kreditkartenkontonummernfeldes liegen. Im vorliegenden Beispiel mit K1 = 5 werden die Zeichen 5 bis 13 ausgewählt.

Der zweite Prüfschlüssel K2 bestimmt, welche Zahlen innerhalb der persönlichen Kennummer durch Angabe der Stellenposition zu prüfen sind, an der die Prüfung beginnen soll. Somit ergäbe k2 = 1 die Prüfung der Stellen 1-6, k2 = 4 die Prüfung der Stel-

len 4-6 und bei k2 = 6 würde nur die wertniedrigste Stelle geprüft während die Zahl der geprüften Stellen (d. h. k2 kleiner) den Betrugsschutz dadurch vergrößert, daß die Zahl nahelegt, daß die Kennummern für den vom Datenverarbeitungssystem unabhängigen Betrieb höher sind. Die lokal geprüften Stellen müssen jedoch eine vorgegebene Korrespondenz mit der Kreditkarteninformation haben, während die nicht geprüften Stellen eine willkürliche Korrespondenz haben können. Vergrößert man die Zahl der lokal geprüften Stellen, so wird dadurch die Anzahl von Stellen verkleinert, die für eine willkürliche Korrespondenz zur Verfügung stehen und die Möglichkeit des Zugangs zur Datenbasis einer angeschlossenen Datenverarbeitungsanlage für den Fall vergrößert, daß der Korrespondenzalgorithmus und der Codierschlüssel gefährdet werden. Im vorliegenden Beispiel wird weiter angenommen, daß der Kunde sein Wahlrecht ausgeübt hat durch Auswählen der lokalen Prüfeinrichtung mit k2 = 4.

Der bestimmte Verschlüsselungsalgorithmus, die die Korrespondenz zwischen der Kennzahl und der Kreditkarteninformation bestimmt, ist für die Praxis der Erfindung nur insofern kritisch, als die Beziehung zwischen der Klartexteingabe und dem verschlüsselt ausgegebenen Text abhängig sein sollte von einem Codierschlüssel, der hier als erstes Codierschlüssel, Schlüssel A bezeichnet ist. Als Beispiel wird angenommen, daß der Codieralgorithmus zum Typ Luzifer gehört, wie er beschrieben ist in einem Artikel "Cryptography and Computer Privacy", Scientific American, May 1973, pp. 15-23, oder im Artikel von C. H. Meyer, "Enciphering Data for Secure Transmission", Computer Design, April 1974, pp. 129-134. Ein Codierschlüssel wie z. B. der Schlüssel A für den Algorithmus 106 ist ein Wort, welches 64 binäre Zahlen enthält. Man kann sich den Codierschlüssel auch als 8 Bytes von je acht Bits vorstellen. Der Schlüssel A wird im Hilfsspeicherteil des Funktionsuntersystems 76 gespeichert und belegt acht der 128 Wörter in diesem Speicher. Um diesen Schlüssel vollständig zu schützen, wird er jedesmal zerstört, wenn eine Wartungsfunktion von der Kunden-Interfacetafel angefordert wird. Durch diese Zerstörung wird verhindert, daß gewöhnliches Wartungspersonal Zugriff zum

Code bekommt. Bei einer Anordnung wartet ein vertrauenswürdiger Bankangestellter, der Zugang zum Schlüssel A hat, bis das Wartungspersonal die Wartung der Station beendet hat und gibt dann den 64 Bit großen Code als acht sequentiell eingegebene hexadezimale Zahlenpaare ein. Eine hexadezimale Bildanzeige an der Bedienertafel zeigt die eingegebenen Zahlen an, um bei Bedarf Korrekturen zu ermöglichen, wobei nur die beiden zuletzt eingegebenen Zahlen jeweils angezeigt werden. Diese Einschränkung der Anzeige auf zwei Zahlen schützt die Sicherheit des Schlüssels, weil eine Person, die den Schlüssel zu kopieren versucht, zur Beobachtung der ganzen Anzeige die Bildanzeige eine beträchtliche Zeit beobachten muß. Dadurch wird es unmöglich gemacht, den ganzen Schlüssel in einem Moment bei seiner Eingabe zu beobachten. Wenn der Schlüssel einmal eingegeben ist, kann er nicht mehr im Bild angezeigt werden. Somit kann der Schlüssel A direkt in die Station eingegeben werden.

In einem anderen Beispiel erhält der vertrauenswürdige Bankangestellte nicht den Schlüssel A sondern einen Schlüssel A', der zum Schlüssel A in einer vorgegebenen Beziehung steht. In diesem Falle gibt der vertrauenswürdige Angestellte den Schlüssel A' in die Datenstation genauso ein, als ob er den Schlüssel A eingeben würde. Die Station verarbeitet jedoch den Schlüssel A' nach einem Verschlüsselungsalgorithmus 108, der ähnlich oder auch identisch sein kann mit dem Verschlüsselungsalgorithmus 106, und erzeugt den Codeschlüssel A. Der Verschlüsselungsalgorithmus 108 benutzt einen zweiten Schlüssel C, der ein Stationsrückgriffschlüssel im Codierprozess ist und den Schlüssel A' in den Schlüssel A umwandelt. Es kann auch ein völlig separater Schlüssel bei der Initialisierung für diesen Zweck geladen werden.

Wegen der vorgegebenen Beziehung zwischen den 32 Bits der Kreditkartendaten, die mit dem Schlüssel A verschlüsselt werden, und der sechsstelligen persönlichen Kennnummer, die eine Person bei der Ausgabe der Kreditkarte erhält, ist die Sicherheit des

Schlüssels A extrem wichtig. Wenn eine Klasse von Kreditkarten an mehr als einer Zweigstelle der Kundenbank benutzbar sein soll, dann muß mindestens eine Person an jeder Bank Zugang zum Schlüssel A haben, so daß er bei Bedarf in eine Station 46 eingetastet werden kann. Für eine große Bank mit vielen Zweigstellen kann diese Verteilung sehr weit gehen. Wenn eine Kreditkarte außerdem bei mehr als einer Bank im Austausch benutzbar sein soll, müssen alle die Karte akzeptierenden Banken denselben Schlüssel A haben. Somit haben noch mehr Personen Zugang zum Schlüssel A und das kann ein sehr wesentlicher Punkt werden. Die Benutzung des verschlüsselten Algorithmus 108 bietet eine Sicherheit gegen diese weite Verteilung des Schlüssels A. Durch Verwendung eines Differenzschlüssels C an jeder Bankeinheit arbeitet nur ein vorbestimmter Schlüssel A' entsprechend einem gegebenen Schlüssel C zufriedenstellend und erzeugt den so wichtigen Schlüssel A. Jede Einheit kann z. B. eine separate Bankzweigstelle sein mit drei oder vier Stationen 14. Nur der Schlüssel A' für diese Einheit oder Bankzweigstelle erzeugt de Schlüssel A in zufriedenstellender Weise. Wenn eine Person Zugang zum Schlüssel A' an einer Zweigstelle hat und zu einer anderen Zweigstelle geht, wo ein anderer Schlüssel C im Verschlüsselungsalgorithmus 108 verwendet wird, erzeugt der Schlüssel A' von der ersten Zweigstelle den Schlüssel A an der zweiten Zweigstelle nicht. Somit kann man die Verteilung des Schlüssel A auf eine sehr kleine stark ausgewählte Gruppe von Leuten beschränken. Der Verschlüsselungsalgorithmus 106 erzeugt so als Ausgabe 32 binäre Zahlen, die in einer vorbestimmten Beziehung zu den 32 Eingabebits stehen. Diese 32 Ausgabebits werden in sechs Wörter à 5 Bits in einem Tabellenumwandlungsprozeß 110 unterteilt, wobei nur 30 Bits benutzt werden. Die Wörter können z. B. aus den ersten sechs Gruppen fünf sequentieller Bits gebildet werden, wobei jeweils die beiden letzten Bits nicht benutzt werden. Jede Gruppe von 5 Bits wird im Tabellenumwandlungsprozeß 110 als Adreßwort zur Adressierung einer Tabelle benutzt, die eine Dezimalzahl mit dem Wert zwischen 1 und 9 an jeder Adreßstelle speichert. Die Tabellenumwandlung

ergibt somit sechs Zahlen mit einem Wert jeweils zwischen 1 und 9. Diese Zahlen haben eine direkte Entsprechung zur persönlichen Kennummer und die Zahl 0 ist ausgeschlossen, um persönliche Kennummern zu vermeiden, die mit führenden Nullen beginnen und Verwirrung bei Eingaben mit veränderlicher Länge schaffen können.

Wenn die Information auf der Kreditkarte in Ordnung befunden wird, wird eine Benutzerzugangstafel geöffnet, damit der Benutzer Zugang zur Benutzerbildanzeige und zur Benutzertastatur 112 erhält. Der Benutzer wird angewiesen, seine persönliche Kennummer über das Zahlenfeld der Tastatur einzugeben. Wenn der Benutzer nicht genau sechs Zahlen innerhalb einer vorgegebenen Zeit eingibt, wird eine falsche Kennummer angenommen und ein neuer Versuch vorgeschlagen. Bei Eingabe von genau sechs Zahlen wird ein Teil der eingegebenen persönlichen Kennummer oder auch die ganze Nummer wahlfrei mit der durch die Tabellenumwandlung 110 erzeugten sechsstelligen Zahl verglichen. Der Schlüssel k2 gibt an, welches der sechs entsprechenden Zahlenpaare zu vergleichen ist.

In diesem Beispiel wurde angenommen, daß k2 = 4 ist, so daß die drei wertniedrigsten Stellen mit den Positionen 4, 5 und 6 im Vergleichsschritt 114 verglichen werden. Wenn der Vergleich ungültig ist, wird eine falsche Kennummer angezeigt und der Benutzer aufgefordert, die Kennummer noch einmal einzugeben. Wenn bei einer gegebenen Anzahl von Wiederholungen, beispielsweise drei Wiederholungen, die persönliche Kennummer nicht richtig eingegeben wurde, wird die Transaktionsanforderung beendet und eine Nachricht an das Datenverarbeitungssystem gegeben. Auf Befehl der Datenverarbeitungsanlage wird die Kreditkarte vorzugsweise in einen Rückhaltebehälter transportiert, um zu verhindern, daß durch weitere Benutzung der möglicherweise gestohlenen Kreditkarte in beliebigen Versuchen die persönliche Kennummer doch noch ermittelt wird. Andererseits kann die Kreditkarte auch dem Benutzer zurückgegeben werden. Wenn festgestellt wird, daß die verglichenen Zahlen der eingetasteten persönlichen Kennummer mit den aus der Kreditkarte

erhaltenen entsprechenden Zahl übereinstimmen, werden die sechs Zahlen der persönlichen Kennummer im Schritt 116 in einen 32 Bit großen Binärcode umgewandelt. Im Schritt 116 erhält man die ersten 24 Bits direkt aus den sechs eingegebenen Zahlen. Die letzten acht Bits oder das erste Byte erhält man durch Behandlung jedes sequentiellen Paares aus vier Bitzahlen als ein Byte und Benutzung der nachfolgenden Antivalenzverknüpfung entsprechender Bitpositionen jedem resultierenden Bytes, so daß man den Dateninhalt der entsprechenden Bitposition im vierten Byte erhält. Andere Wege zur Erhaltung der letzten acht Informationsbits sind so lange akzeptabel, wie das Verfahren zu einer veränderlichen Information führt, die eine Funktion aller Bits der eingegebenen persönlichen Kennummer sind. Diese 32 Bits werden dann mit einem Verschlüsselungsalgorithmus 118 verarbeitet, der den Schlüssel A zur Erzeugung einer verschlüsselten 32 Bit großen persönlichen Kennummer benutzt. Der Verschlüsselungsalgorithmus 118 kann im allgemeinen jeder gegeignete Verschlüsselungsalgorithmus sein, für dieses Beispiel wird jedoch angenommen, daß er mit dem Verschlüsselungsalgorithmus 106 identisch ist. Die Benutzung desselben Algorithmus für beide Verschlüsselungsprozesse gestattet die Verwendung desselben gespeicherten Programmes oder der Maschinenlogik für beide Prozesse. Der Codierschlüssel für den Algorithmus 118 kann im allgemeinen auch jeder gegeignete Schlüssel sein, für dieses Beispiel wird jedoch angenommen, daß der Algorithmus 118 den Schlüssel A verwendet, der mit dem für den Algorithmus 106 verwendeten Schlüssel A identisch ist. Diese mehrfache Benutzung desselben Schlüssels und desselben Verschlüsselungsalgorithmus reduziert die Komplexität im Betrieb der Station 14 und die Größe des benötigten Datenspeichers weiter. Die aus dem Verschlüsselungsalgorithmus 118 resultierenden 32 Bits stellen somit eine einmal verschlüsselte persönliche Kennummer dar.

Die 32 Bits der verschlüsselten persönlichen Kennummer werden dann im Schritt 120 in sechs 4 Bit große Zahlen umgewandelt, wo-

bei zwei 4 Bit große Zahlen fallengelassen werden. Im Schritt 122 werden die beiden ausgeschiedenen Zahlen ersetzt durch zwei 4 Bit große Zahlen veränderlicher Daten. Dieser Austausch, der von der Kennummer abgeleiteten Information durch veränderliche Information verhindert, daß das verschlüsselte Feld konstant ist. Im allgemeinen können die veränderlichen Daten irgendwelche Daten sein, die keine vorgegebene Beziehung zur persönlichen Kennummer haben und sich mit jeder Transaktionsanforderungsnachricht ändern. Im Ausführungsbeispiel bestehen diese veränderlichen Daten aus der Bargeldzählerzahl für die Bargeldausgabetransaktionen und einer Transaktionszahl für andere Transaktionen.

Die aus der Kombination der sechs 4 Bit großen Zahlen und der acht Bits veränderlicher Daten resultierenden 32 Bits werden dann durch einen Verschlüsselungsalgorithmus 124 geleitet, der einen dritten Schlüssel B benutzt. Der Verschlüsselungsalgorithmus 124 kann im allgemeinen jeder geeignete Verschlüsselungsalgorithmus sein, für dieses Ausführungsbeispiel wird jedoch angenommen, daß der Algorithmus 124 identisch ist mit den Algorithmen 118, 106 und 108. Der Schlüssel B ist 64 Bits groß und wird vom Datenverarbeitungssystem 12 während der Initialisierung empfangen. Er kann nur durch Kommunikation eines neuen Schlüssels vom Datenverarbeitungssystem geändert werden. Der Verschlüsselungsalgorithmus 124 resultiert in 32 Bits verschlüsselter Daten, die in eine Transaktionsanforderungsnachricht unmittelbar hinter das 4 Byte große allgemeine Vorlauffeld gesetzt werden, wie es oben bereits beschrieben wurde.

Nachdem im Vergleicherschritt 114 die Kreditkarte wenigstens teilweise als gültig erkannt wurde, wird der Benutzer angewiesen, über die Tastatur 112 die Transaktion anzugeben, die er auszuführen wünscht. Zuerst wird der Benutzer angewiesen, die angeforderte Art der Transaktion anzugeben und alle Hinterlichter im Transaktionsanforderungsfeld der Tastatur leuchten auf. Wenn eine bestimmte Taste, in diesem Fall die Betragsübertragungstaste, betätigt wird, leuchtet das Hinterlicht der betätigten Taste

weiter während die Hinterlichter aller anderen Tasten im Feld verlöschen. Der Benutzer wird dann angewiesen, das Konto zu wählen, von dem Beträge zu übertragen sind und die Hinterlichter aller Tasten im Abgangskontofeld leuchten auf. Wenn der Benutzer die Taste "vom Sparkonto" wählt, leuchtet das Hinterlicht dieser Taste weiter während die Hinterlichter aller anderen Tasten im Abgangskontofeld verlöschen. Dann erhält der Benutzer die Anweisung, das Zugangskonto zu wählen, auf das die Beträge zu übertragen sind, und alle Hinterlichter im Zugangskontofeld leuchten auf. Bei Wahl der Scheckkontotaste leuchtet die betätigte Taste weiter und die Hinterlichter aller anderer Tasten im Zugangskontofeld verlöschen. Die leuchtend gebliebenen Hinterlichter gestatten dem Benutzer eine Verfolgung des Vorganges, so daß er den Zustand seiner Transaktionsanforderungseingabe bestätigen oder noch einmal für sich wiederholen kann. Er kann seine Angaben jederzeit dadurch ändern, daß er zu einem vorher bereits eingegebenen Feld zurückkehrt und eine neue Taste betätigt und dann mit der Eingabe über Tastatur von diesem Punkt an fortfährt. Numerische Information wie die zu übertragenen Dollarbeträge, werden durch das numerische Feld der Tastatur 112 eingegeben. Die gesamte eingegebene numerische Information wird mit Ausnahme der persönlichen Kennummer im Bild angezeigt. Diese Kennummer wird nicht angezeigt, um die unberechtigte Kenntnisnahme von dieser Nummer durch eine hinter dem Benutzer stehende Person zu vermeiden. Die Tastaturdaten, die vom Magnetstreifen gelesenen Kreditkartendaten und alle gewünschten zusätzlichen Daten werden dann im Klartext hinter das 4 Byte große allgemeine Vorlauffeld und das 4 Byte große codierte Feld gesetzt. Diese Information wird dann dem Datenverarbeitungssystem 12 als Transaktionsanforderungsnachricht übermittelt.

2. TRANSAKTIONSANTWORTNACHRICHT

Wenn von dem in Fig. 4 gezeigten Datenverarbeitungssystem 12 eine Transaktionsanforderungsnachricht empfangen wird, durchläuft sie die Verarbeitung 140 in verschiedene Datenfelder, deren gemein-

sames Vorlauffeld zur Nachrichtenführung benutzt wird. Die 32 verschlüsselten Bits werden durch einen Entschlüsselungsalgorithmus 142 geleitet und der Klartext vom Datenprozessor 144 empfangen, der einen großen Datenspeicher 146 hat. Der Entschlüsselungsalgorithmus 142 benutzt denselben Schlüssel B wie der Verschlüsselungsalgorithmus 124. Die Datenverarbeitungsanlage 12 adressiert mit den Klartextdaten die Datenbasis des Benutzers (Datei) im Datenspeicher 146. Diese Datei enthält Kontodaten sowie zur Kreditkarte des Benutzers gehörende Information wie beispielsweise die verschlüsselte persönliche Kennummer.

Die durch den Verschlüsselungsalgorithmus 142 erzeugten 32 Bits werden durch einen Trennprozessor 144 geleitet, wo die sechs 4 Bit großen Stellen der verschlüsselten persönlichen Kennummer von den beiden veränderlichen Zahlen getrennt werden. In dem anschließenden Vergleich 148 werden die übermittelten sechs Zahlen der verschlüsselten Kennummer verglichen mit den sechs Zahlen der Verschlüsselungsinformation aus der Datei, die in verschlüsselter Form gespeichert wurde.

Dieser Verschlüsselungsprozess verbessert die Sicherheit der in verschiedenen Transaktionsstationen 14 gespeicherten Bargeldmengen, wobei diese Stationen in Kommunikation mit einem angeschlossenen Datenverarbeitungssystem stehen können. Wenn jemand mit bösen Absichten im Besitze der Korrospondenz zwischen Kreditkartenkontonummern und persönlicher Kennummer ist, kann er betrügerischerweise Bargeld von der Station 14 erhalten. So kann jemand beispielsweise Kreditkarten fälschen oder stehlen, auf denen Information gespeichert ist, die mit echten Benutzerkonten zu tun hat. Unter Verwendung der gefälschten Kreditkarte und der entsprechenden persönlichen Kennummer kann eine Person erst den Stand der verschiedenen Sparkonten, Scheckkonten oder anderer Konten erfragen, die durch die Kreditkarte zugänglich sind. Wenn er dann über den Kontostand informiert ist, kann er mit Hilfe der Kreditkarte und der Bargeldausgabestation 14 Bargeld von den Konten abheben, bis

entweder die Konten oder die Bargeldstation leer sind. Weitere Konten könnten mit ihrer Kreditkarte und den entsprechenden persönlichen Kennummer auf ähnliche Weise benutzt werden, bis das gesamte Bargeld an einer Bargeldausgabestation ausgegeben worden ist. Die betreffende Person kann dann das Bargeld von weiteren Bargeldausgabestationen im System mit weiteren Kreditkarten und persönlichen Kennummern abheben. Da jede Bargeldstation 14 einige Tausend Dollar enthalten kann und viele Stationen 14 mit dem Datenverarbeitungssystem in Kommunikation stehen, wird es extrem wichtig, die Korrospondenz zwischen Kreditkartenkontonummern und persönlichen Kennummern gesichert zu halten und doch für eine höhere Verfügbarkeit der Stationen 14 im unabhängigen Betrieb lokale Prüfungen zu ermöglichen. Es wird extrem schwierig, sich die Korrespondenz zwischen der Kreditkarteninformation und der persönlichen Kennummer für eine große Anzahl von Konten zu verschaffen, wenn die hier beschriebenen Techniken angewandt werden. Auch wenn die persönliche Kennummer dadurch vollständig erzeugt werden kann, daß mit die gespeicherte Kreditkarteninformation durch den Verschlüsselungsalgorithmus 106 laufen läßt, wird die Sicherheit des Codierschlüssels A gemäß obiger Beschreibung trotzdem aufrecht erhalten.

Wenn die Relation eines Teiles (oder vorzugsweise aller) der ersten drei Zahlen der persönlichen Kennummer und der gespeicherten Kreditkarteninformation nicht vorher festgelegt ist, wird es noch schwieriger, das ganze System zu betrügen. Es besteht die Möglichkeit, daß Personal am Datenverarbeitungszentrum für das Datenverarbeitungssystem Zugang zu der gespeicherten verschlüsselten Kennummer hat. Die tatsächliche persönliche Kennummer ist jedoch im Datenverarbeitungssystem nicht gespeichert und die codierte Kennummer ist wertlos, wenn man Bargeld von einer Station 14 bekommen will, da die eigentliche persönliche Kennummer über die Tastatur einer Station 14 eingegeben werden muß. Wenn also jemand die Korrespondenz zwischen einer großen Anzahl von Kreditkarten und den entsprechenden persönlichen Kennummern haben will, muß er Zugriff sowohl zur verschlüsselten persönlichen Kennummer haben,

die in Datenbasis gespeichert ist, als auch zum Entschlüsselungsalgorithmus, der dem Verschlüsselungsalgorithmus 118 und dem Schlüssel A entspricht.

Bei der Ausgabe von Kreditkarten kann die Kenntnis der Korrespondenz zwischen den Kreditkartendaten und der persönlichen Kennummer auf wenige Leute beschränkt werden. Es lassen sich tatsächlich Konten einrichten, bei denen ein Teil der persönlichen Kennummer aus der Kreditkarteninformation abgeleitet wird und ein anderer Teil wahlfrei von einem Computer erzeugt wird. Die gesamte persönliche Kennummer kann dann ausgedruckt und in einem Umschlag zusammen mit einer Kreditkarte versiegelt werden, so daß die persönliche Kennummer dem menschlichen Auge nur zugänglich ist, nachdem der Umschlag dem künftigen Benutzer bei Eröffnung eines Kreditkartenkontos, das durch eine Station 14 bearbeitet werden kann, übergeben wurde. Auf diese Weise kann ein Zuordnungssystem entwickelt werden, in dem kein Bankangestellter Zugang zu der Korrespondenz zwischen den Kreditkartenkonten und der zugehörigen persönlichen Kennumer hat.

Wenn im Vergleich 150 festgestellt wird, daß die gespeicherte und die übertragene verschlüsselte persönliche Kennummer nicht identisch sind, setzt das Datenverarbeitungssystem eine Transaktionsantwortnachricht zusammen und überträgt sie, die anzeigt, daß die Ausführung der Transaktion nicht genehmigt wird. Die Transaktionsantwortnachricht kann die anfordernde Station 14 beauftragen, die Benutzerkreditkarte entweder einzuziehen oder zurückzugeben. Wenn andererseits die gespeicherte und die übermittelte codierte Kennummer einander entsprechen und die angeforderte Transaktion vorgegebene Regeln, die sich auf Dollarbeträge, Abhebungsgrenzen oder Kontostände beziehen, nicht verletzt, wird die Transaktion durch eine Transaktionsantwortnachricht genehmigt. Die Transaktionsantwortnachricht enthält 32 Bits codierter Information, die den 32 Bits der codierten Information entsprechen, die in der Transaktionsanforderungsnachricht empfangen wurden. Im Zusammensetzungsprozess 152 werden 32 Bits zur Verschlüsselung mit dem

Verschlüsselungsalgorithmus 154 unter Verwendung des Schlüssels B, des dritten Übertragungsschlüssels, zusammengesetzt. Der Verschlüsselungsalgorithmus kann im allgemeinen jeder geeignete Verschlüsselungsalgorithmus sein, für dieses Beispiel wird jedoch angenommen, daß der Algorithmus mit den Verschlüsselungsalgorithmen 106, 118 und 124 identisch ist. Es wird weiter angenommen, daß für diese Verschlüsselung derselbe Schlüssel B verwendet wurde wie für den Verschlüsselungsalgorithmus 124. Die 32 zur Verschlüsselung zusammengesetzen Bits, unterscheiden sich von den übertragenen 32 Bits, die die sechs Zahlen der verschlüsselten persönlichen Kennummer und zwei veränderliche Zahlen enthielten. Die 32 Bits der Transaktionsantwortnachricht enthalten ein Byte für die Bargeldzählerzahl entsprechend einer ersten Bargeldzahl (CNTR1), die von einer Station 14 gehalten wird und für jede ausgegebene Rechnung erhöht wird, ein Aktionsbyte, welches die Antwort für die Station 14 auf die angeforderte Benutzertransaktion darstellt, ein zweites Bargeldzählerbyte (CNTR2), welches die Bargeldzahl angibt, die für eine zweite Bargeldausgabeeinrichtung in der Station 14 gehalten wird und ein Betragsbyte (AMT), welches die Anzahl von für die angeforderte Transaktion relevanten Rechnungen angibt. Diese 32 Bits werden dann durch den Verschlüsselungsalgorithmus 254 zu 32 verschlüsselten Bits 156 verarbeitet. Die verschlüsselten Bits 156 werden dann mit Klartextdaten, wie beispielsweise wahlfreien Bildanzeigedaten, wahlfreien Empfangsdaten oder zusätzlichen Daten kombiniert, die zur Beendigung der Transaktion notwendig sind und an die anfordernde Station 46 als Transaktionsantwortnachricht im Schritt 158 zurückübertragen.

3. AUSFÜHRUNGS- UND ZUSTANDSNACHRICHT

Wenn die Transaktionsantwortnachricht an der Station 14 empfangen wird, durchläuft sie die Eingangsverarbeitung 160, um die Übertragungsgenauigkeit zu prüfen und die Antwortnachricht in ihre verschiedenen Felder aufzuteilen. Das verschlüsselte Feld wird durch einen Entschlüsselungsalgorithmus 162 geleitet, der unter

Verwendung des Schlüssels B die 32 Bits wieder herstellt, die die Bargeldzählerzahl 1 (CNTR1), die Aktion, die Bargeldzählerzahl 2 (CNTR2) und die Betragsdaten (AMT) enthalten. Diese Bytes werden auf Genauigkeit geprüft, um sicherzustellen, daß die Transaktionsantwortnachricht fehlerfrei empfangen wurde und der richtigen Transaktionsanforderungsnachricht entspricht. Ein Transaktionsabschluß 164 wird dann nach dem Inhalt der Transaktionsantwortnachricht ausgeführt. Beim Abschluß einer Transaktion gibt die Station 14 die Kreditkarte zurück oder zieht sie ein, gibt entsprechende Belege aus wie Bestätigungen über Bargeldausgabe oder eine Transaktion, führt die Transaktion formell aus oder annuliert sie, zeigt entsprechende Nachrichten zur Genehmigung oder Ablehnung durch den Kunden auf dem Bildschirm an und übernimmt weitere Transaktionsausführungsfunktionen, die zum Abschluß der Transaktion notwendig sind.

Beim Abschluß einer vom Benutzer angeforderten Transaktion sendet die Station 14 eine Zustandsnachricht an das Datenverarbeitungssystem 12, die diesen den Zustand der Station 14 mitteilt und wie die angeforderte Transaktion beendet wurde. Die Vorbereitung der Zustandsnachricht enthält die Zusammensetzung 166 von 32 Bits, die mit dem Verschlüsselungsalgorithmus 168 und dem Schlüssel B zu 32 verschlüsselten Bits 170 zusammengesetzt werden. Der Verschlüsselungsalgorithmus kann im allgemeinen jeder geeignete Verschlüsselungsalgorithmus sein, für das Ausführungsbeispiel wird jedoch angenommen, daß der Verschlüsselungsalgorithmus 168 mit den Verschlüsselungsalgorithmen 106, 108, 118, 124 und 154 und der Schlüssel B mit dem für die Verschlüsselungsalgorithmen 124 und 152 verwendeten Schlüssel B identisch ist. Im Gegensatz zum Schlüssel A kann der Schlüssel B jedoch durch das Datenverarbeitungssystem 12 verändert werden und es wird angenommen, daß dies von Zeit zu Zeit geschieht. Die 32 Bits 170 durchlaufen die Ausgabeverarbeitung 172, während sie mit nicht verschlüsselter Zustandsinformation kombiniert und als Zustandsnachricht von der Transaktionsausführungsstation 14 an das Datenverarbeitungssystem 12

übertragen werden.

Das hier beschriebene Benutzungsverfahren für Verschlüsselungsalgorithmen bietet eine große Sicherheit für das Transaktionsausführungssystem 10, ohne daß große Speicherkapazität zum Speichern mehrerer Verschlüsselungsprogramme gebraucht wird. Bei richtiger Auswahl der Verschlüsselungs- und Entschlüsselungsalgorithmen kann der Entschlüsselungsalgorithmus außerdem dem Verschlüsselungsalgorithmus sehr ähnlich sein, um eine doppelte Benutzung des größten Teiles des Verschlüsselungsalgorithmusprogrammes für Verschlüsselung und Entschlüsselung zu ermöglichen. Das führt zu weiteren Einsparungen beim notwendigen Programmspeicherplatz. Die letzte Verschlüsselung der 32 Bits der verschlüsselten Information in den drei Benutzertransaktionsnachrichten gestattet eine Sicherung der verschlüsselten persönlichen Kennummer zusammen mit dem Kommunikationskanal, während dadurch gleichzeitig die Benutzung desselben allgemeinen Formates für alle drei Nachrichten ermöglicht wird. In der Transaktionsanforderunsnachricht kombiniert der Zusammensetzungsprozess 122 die verschlüsselte persönliche Kennummer mit unterschiedlichen Daten, um es einer die Kommunikationsleitungen überwachenden Person extrem schwierig zu machen, den Schlüssel B und den Verschlüsselungsalgorithmus 124 dadurch zu knacken, daß man wiederholt dieselbe Kennummer, die Kreditkarte und die Anforderung eingibt und die entsprechenden verschlüsselten Kommunikationen überwacht. Die Transaktionsantwortnachricht enthält ein Zählerbyte 1, ein Aktionsbyte, ein Zählerbyte 2 und einen Betrag. Diese Information ist vollständig verschieden von der codierten Information der Transaktionsanforderungsnachricht und enthält außerdem veränderliche Information. Der Betrag und das Aktionsbyte sind zwar für dieselben Arten von Transaktionsanforderung so ziemlich dieselben, die Kontrollbytes ändern sich jedoch. Die 32 verschlüsselten Bits der Zustandsnachricht unterscheiden sich von den verschlüsselten Feldern einer der beiden Nachrichten dadurch, daß sie die Transaktionszahl enthalten, die sich mit der Zeit ändert, die Bytes für den Zähler 2

und den Zähler 1 an anderen Bytepositionen als die Transaktionsantwortnachricht und ein Zahlenbyte (CB), welches über eine binäre Zählerangabe die Anzahl der auf den verschlüsselten Teil der Nachricht für eine normale Zustandsnachricht folgenden Zustands- und Anfragedatenbytes angibt. Eine aufgrund einer Transaktionsbeendigung erzeugte Zustandsnachricht enthält normalerweise kein Anfragedatenbyte. Falls die Zustandsnachricht eine Anforderungswiederholung der Ausnahmezustandsnachricht ist, enthält das dritte Byte (CB) des Verschlüsselungsfeldes das Aktionsbyte aus der Transaktionsantwortnachricht für die letzte Anforderung. Durch Veränderung des Schlüssels B von Zeit zu Zeit und Übertragen anderer Information in den verschlüsselten Teil eines anderen Nachrichtentyps wird das Knacken des Übertragungsverschlüsselungsalgorithmus und das Herausfinden des augenblicklich gültigen Schlüssels B durch Überwachung der Kommunikationsleitungen extrem schwierig gestaltet. Auch wenn der Übertragungsverschlüsselungsalgorithmus und der Schlüssel B geknackt werden, läßt sich durch Überwachung der Nachrichtenübertragungen eine Korrespondenz zwischen Konten und verschlüsselter persönlicher Kennummer nur für bestimmte Kreditkarten herstellen, die während der Überwachung der Kommunikation benutzt werden. Größere Mengen gestohlener oder gefälschter Kreditkarten und der entsprechenden persönlichen Kennummern lassen sich nur durch weiteres Knacken des Schlüssels A zusammenstellen. Bei einem anderen Ausführungsbeispiel, bei dem zwischen allen Zahlen der persönlichen Kennummer und der Information auf der Kreditkarte eine vorgegebene Beziehung besteht, ist ein Zugriff zur Datenbasis nicht notwendig. Die Schlüssel k1 und k2 liefern natürlich eine weitere Sicherheit für die verschlüsselte persönliche Kennummer, falls die örtliche Kennummernprüfeinrichtung implementiert wird.

PATENTANSPRÜCHE

1. Kommunikationssystem mit mißbrauchgeschützter, zentraler Kontendatei, mit einem zentralen Prozessor (Gastprozessor) und einer Vielzahl von Benutzerterminals mit jeweils einem Tastenfeld und Eingabeeinrichtungen für Schecks, Kreditkarten, und dergl., zur Übertragung von Transaktionsdaten und einer Benutzer-Identifizierungszahl, gekennzeichnet durch einen ersten Codierer (118) zur Verschlüsselung zumindest eines Teiles der Benutzer-Identifizierungszahl (ID), zur Erzeugung eines ersten verschlüsselten Datenblocks (120),
durch einen zweiten Codierer (124) zur Verschlüsselung zumindest eines Teiles des ersten verschlüsselten Datenblocks zur Erzeugung eines zweiten verschlüsselten Datenblocks,
sowie durch mit dem zweiten Codierer verbundenen Einrichtungen (152, 166) zur Erzeugung von mit jeder Transaktion veränderten, variablen Daten.

2. Kommunikationssystem nach Anspruch 1, gekennzeichnet durch Einrichtungen (76) zur Speicherung einer ersten (A) und einer zweiten (B) Verschlüsselungszahl zur Erzeugung jeweils des ersten und des zweiten verschlüsselten Datenblocks.

3. Kommunikationssystem nach Anspruch 2, gekennzeichnet durch einen dritten Codierer (108) zur Erzeugung der ersten Verschlüsselungszahl (A) aus einer dritten, gespeicherten Verschlüsselungszahl (C) und aus einer zusätzlich eingegebenen Verschlüsselungszahl (A').

4. Kommunikationssystem nach Anspruch 1, dadurch gekennzeichnet,
daß der erste Codierer (118) einen Teil der Identifizierungszahl (ID) unverändert übernimmt und den restlichen Teil mit der ersten Verschlüsselungszahl (A) durch eine logische Funktion (z. B. Exclusiv-ODER-Funktion) kombiniert.

5. Kommunikationssystem nach Anspruch 1, gekennzeichnet durch einen vierten Codierer (106) zur Verschlüsselung eines Teiles von auf dem Scheck oder der Kreditkarte fest aufgezeichneten Informationen mit der ersten Verschlüsselungszahl (A), sowie durch eine Auswahleinrichtung (104) zur Auswahl eines Teiles der fest aufgezeichneten Daten.

6. Kommunikationssystem nach Anspruch 5, dadurch gekennzeichnet,
daß die verschlüsselten Ausgangsdaten des vierten Decodierers (106) aus einer Tabelle (110) Zeichen auslesen, die mit der Benutzeridentifizierungszahl (ID) verglichen werden und bei Nichtübereinstimmung die Übertragung des zweiten verschlüsselten Datenblockes zum zentralen Prozessor (144) verhindern können.

7. Kommunikationssystem nach Anspruch 1, dadurch gekennzeichnet,
daß eine Transaktion aus einer vom Terminal (14) zum zentralen Prozessor (16) übertragenen Anforderungsnachricht (Fig. 3), aus einer darauffolgenden Antwortnachricht vom zentralen Prozessor zum Terminal sowie aus einer darauffolgenden Ausführungs- und Statusnachricht besteht, wobei die verschlüsselten Daten der Anforderungsnachricht im zentralen Prozessor in einem ersten Entschlüssler (142) mit Hilfe der zweiten Verschlüsselungszahl (B) entschlüsselt werden, die variablen Daten zum Datenprozessor (144) über-

tragen werden und die hierzu im Datenprozessor gespeicherten Daten mit der Identifizierungszahl vom entschlüsselten Datenblock (148) verglichen werden.

8. Kommunikationssystem nach Anspruch 1, gekennzeichnet durch Zähleinrichtungen (ZLR1) zur Zählung von vom Terminal ausgelieferten Ausgabematerials (z. B. Geldscheine) durch weitere Zähleinrichtungen (ZLR2) zur Angabe des verfügbaren Geldbetrages, wobei beide Zählangaben als variable Daten zur Erzeugung des zweiten verschlüsselten Datenblocks verwendet werden.

9. Kommunikationssystem nach Anspruch 1, dadurch gekennzeichnet, daß die akkumulierte Anzahl von Dokumenten, die von der Ausgabeeinrichtung herausgegeben werden und eine fortlaufende Transaktionszahl als variable Daten verwendet werden.

Leerseite

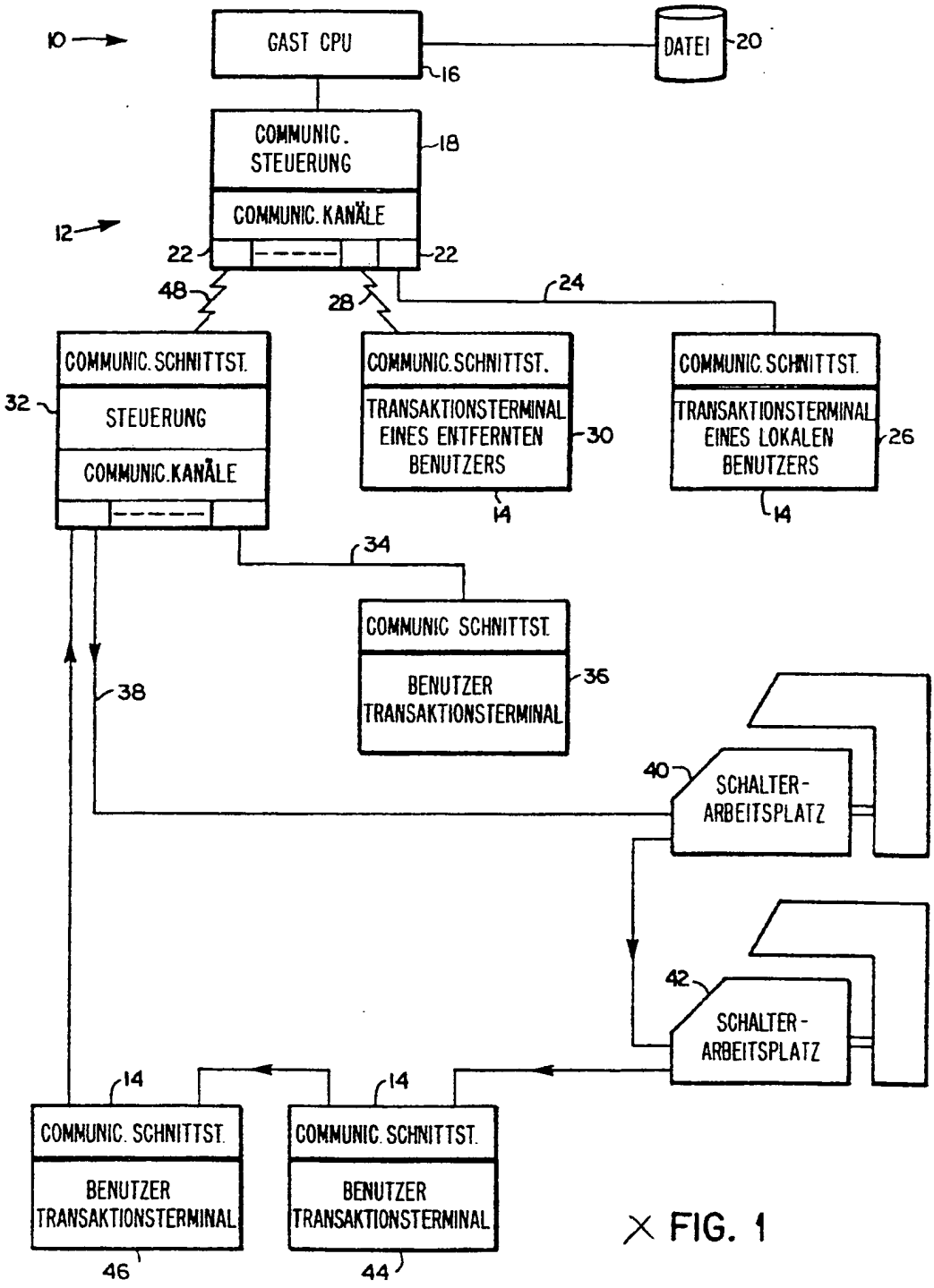

10
GAST CPU
16
DATEI
20
COMMUNIC. STEUERUNG
18
COMMUNIC. KANÄLE
12
22
22
48
28
24
COMMUNIC. SCHNITTST.
STEUERUNG
COMMUNIC. KANÄLE
32
COMMUNIC. SCHNITTST.
TRANSAKTIONSTERMINAL EINES ENTFERNTEN BENUTZERS
30
14
COMMUNIC. SCHNITTST.
TRANSAKTIONSTERMINAL EINES LOKALEN BENUTZERS
26
14
34
COMMUNIC SCHNITTST.
BENUTZER TRANSAKTIONSTERMINAL
36
38
40
SCHALTER-ARBEITSPLATZ
42
SCHALTER-ARBEITSPLATZ
14
14
COMMUNIC. SCHNITTST.
BENUTZER TRANSAKTIONSTERMINAL
46
COMMUNIC. SCHNITTST.
BENUTZER TRANSAKTIONSTERMINAL
44

FIG. 1

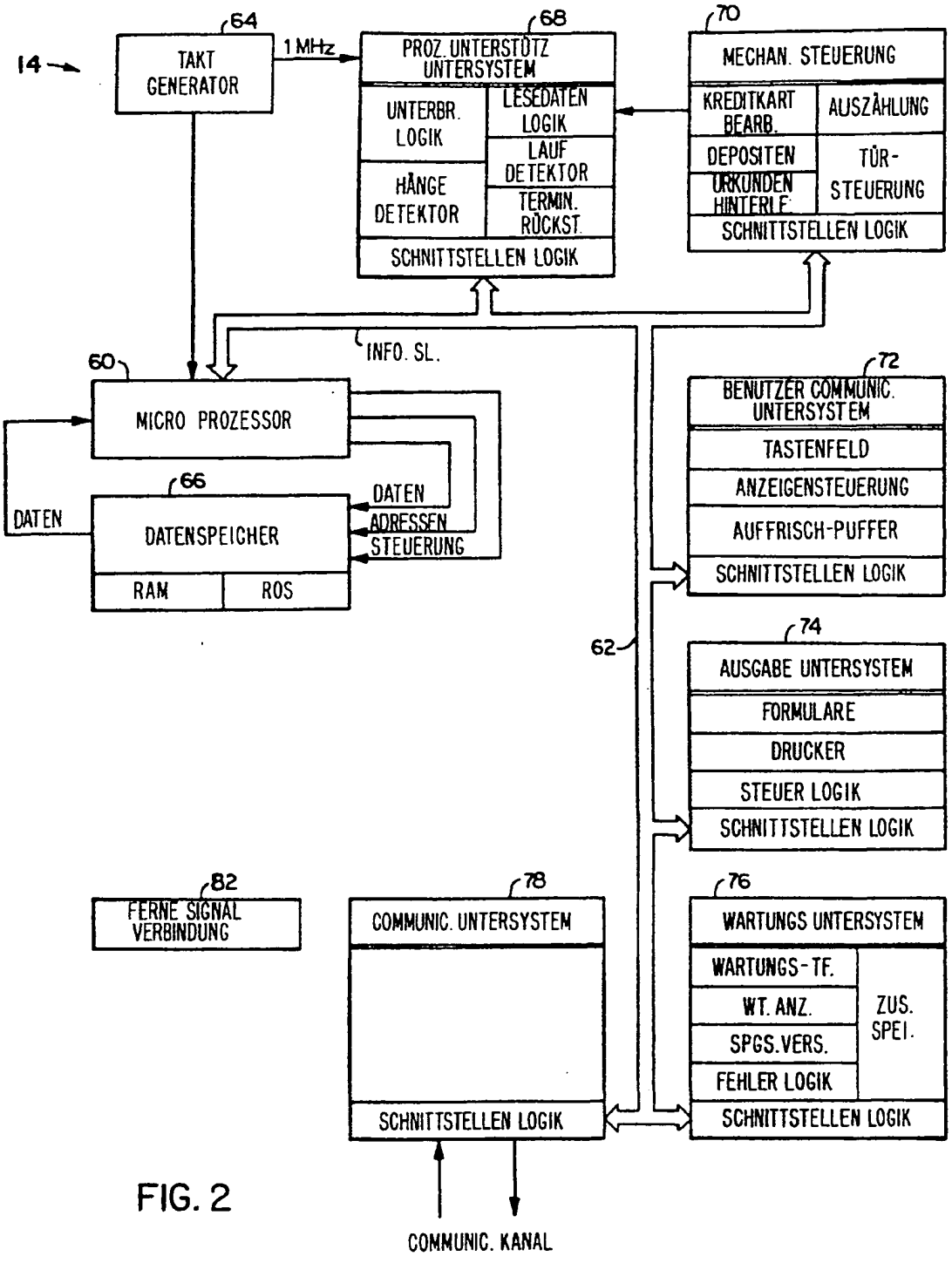
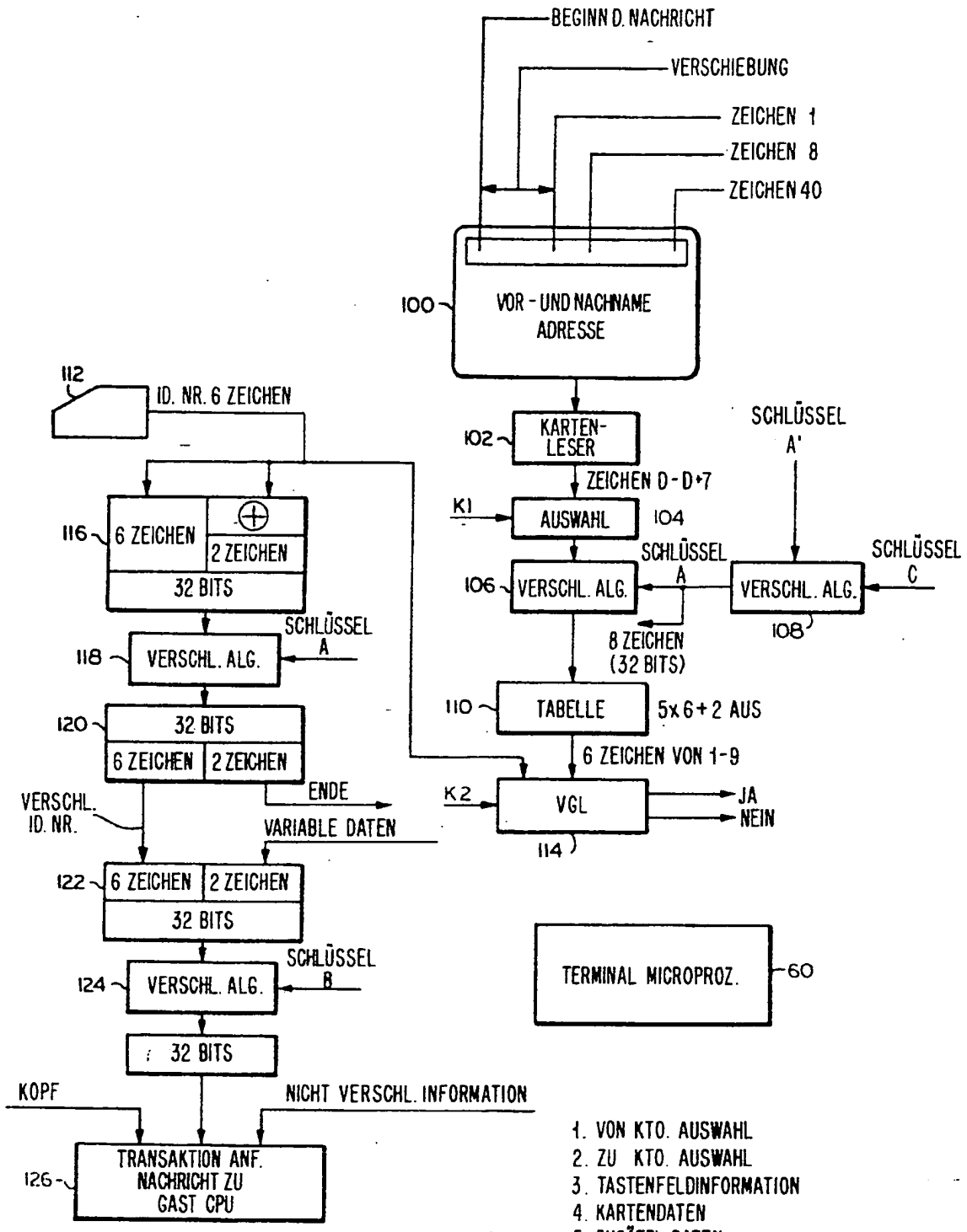

14
64
TAKT GENERATOR
1 MHz
68
PROZ. UNTERSTÜTZ UNTERSYSTEM
UNTERBR. LOGIK
LESEDATEN LOGIK
LAUF DETEKTOR
HÄNGE DETEKTOR
TERMIN. RÜCKST.
SCHNITTSTELLEN LOGIK
70
MECHAN. STEUERUNG
KREDITKART BEARB.
AUSZÄHLUNG
DEPOSITEN
TÜR-STEUERUNG
URKUNDEN HINTERLE.
SCHNITTSTELLEN LOGIK
INFO. SL.
60
MICRO PROZESSOR
66
DATEN
DATENSPEICHER
ADRESSEN
STEUERUNG
RAM
ROS
72
BENUTZER COMMUNIC. UNTERSYSTEM
TASTENFELD
ANZEIGENSTEUERUNG
AUFFRISCH-PUFFER
SCHNITTSTELLEN LOGIK
62
74
AUSGABE UNTERSYSTEM
FORMULARE
DRUCKER
STEUER LOGIK
SCHNITTSTELLEN LOGIK
82
FERNE SIGNAL VERBINDUNG
78
COMMUNIC. UNTERSYSTEM
SCHNITTSTELLEN LOGIK
76
WARTUNGS UNTERSYSTEM
WARTUNGS-TF.
WT. ANZ.
SPGS.VERS.
FEHLER LOGIK
ZUS. SPEI.
SCHNITTSTELLEN LOGIK
COMMUNIC. KANAL

FIG. 2



1. VON KTO. AUSWAHL
2. ZU KTO. AUSWAHL
3. TASTENFELDINFORMATION
4. KARTENDATEN
5. ZUSÄTZL. DATEN

FIG. 3

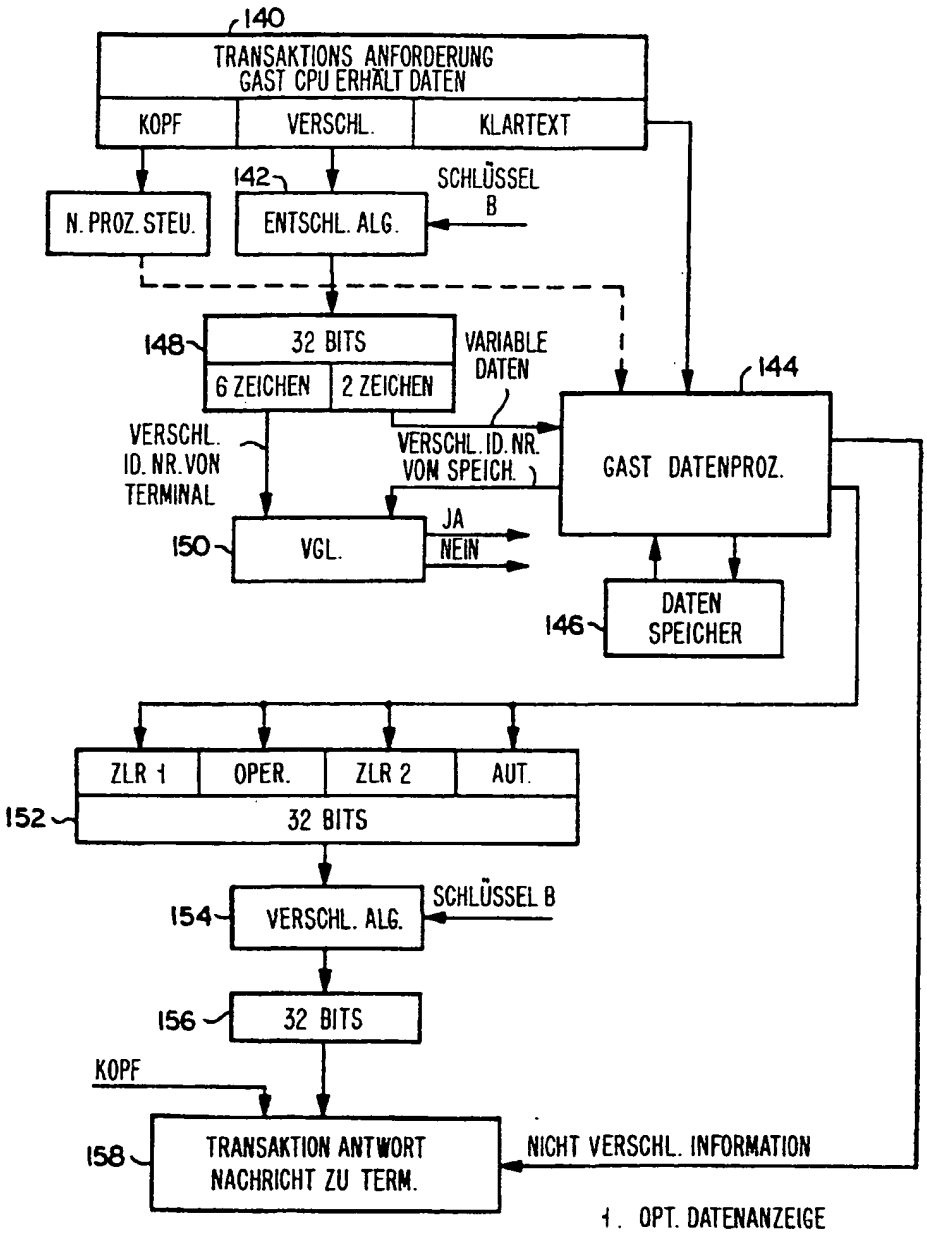

140
TRANSAKTIONS ANFORDERUNG
GAST CPU ERHÄLT DATEN
KOPF
VERSCHL.
KLARTEXT
142
SCHLÜSSEL B
N. PROZ. STEU.
ENTSCHL. ALG.
148
32 BITS
6 ZEICHEN
2 ZEICHEN
VARIABLE DATEN
144
VERSCHL. ID. NR. VON TERMINAL
VERSCHL. ID. NR. VOM SPEICH.
GAST DATENPROZ.
150
VGL.
JA
NEIN
146
DATEN SPEICHER
ZLR 1
OPER.
ZLR 2
AUT.
152
32 BITS
154
VERSCHL. ALG.
SCHLÜSSEL B
156
32 BITS
KOPF
158
TRANSAKTION ANTWORT NACHRICHT ZU TERM.
NICHT VERSCHL. INFORMATION
1. OPT. DATENANZEIGE
2. OPT. DATENEMPFANG
3. ZUS. DATEN

FIG. 4